

**Section 404 exercises
can provide the starting
point for a comprehensive
ERM program.**

NOW THAT YOUR ORGANIZATION'S INITIAL WORK for the U.S. Sarbanes-Oxley Act of 2002 is winding down, what will you do with your team of Section 404 experts? They have worked hard, going through exercises to support the certification of the company's internal controls over financial reporting. The next logical step would be to leverage that investment and implement a total enterprise risk management (ERM) framework. ■ Much was gained from the Sarbanes-Oxley exercise. Senior executives learned the

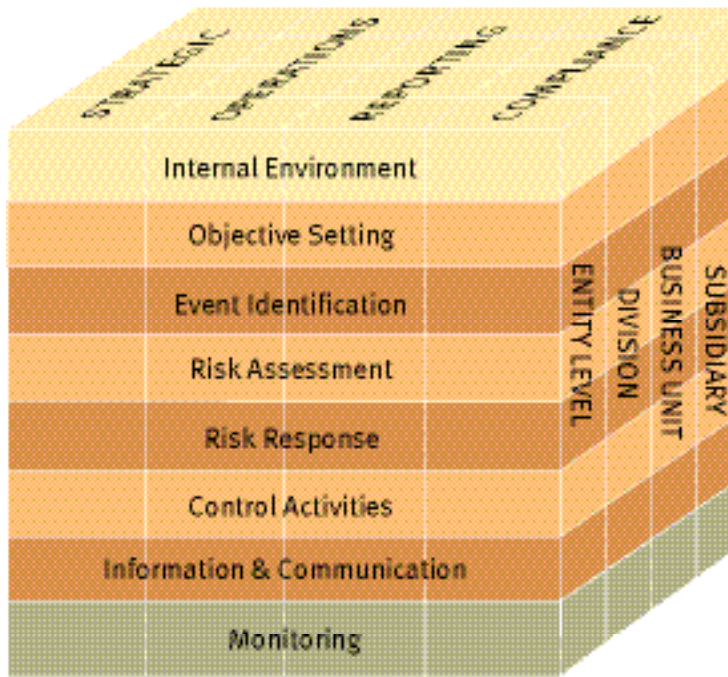
Beyond Sarbanes-Oxley

BY GEORGE MATYJEWICZ, PHD
MANAGING DIRECTOR
D'ARCANGELO SOFTWARE SERVICES

JAMES R. D'ARCANGELO, CPA
MANAGING PARTNER
D'ARCANGELO & COMPANY, LLP.

importance of establishing objectives, identifying risks that will prevent them from meeting those objectives, and establishing controls that will mitigate those risks. Under the act, those objectives translate into disclosure control objectives and procedures for financial statement assertions, including existence, completeness, valuation, rights and obligations, and presentation and disclosure. ■ The chief executive officer (CEO) and chief financial officer (CFO) are required to certify that they have effective internal controls over financial reporting and report whether there have been any significant changes from one quarter to the next. The quarterly evaluation process includes review and testing of controls by appropriate personnel —

COSO ERM Cube



at the proper levels of the enterprise — and signing off that they are in place. Where there are deficiencies or weaknesses, action must be taken to remediate the risk of financial statement misstatement.

The act requires controls to be assessed against a suitable framework such as The Committee of Sponsoring Organizations of the Treadway Commission’s (COSO’s) *Internal Control–Integrated Framework* (IC-IF). The framework consists of three categories — strategic, operations, and reporting — and five components: internal environment, risk assessment, control activities, information and communication, and monitoring. Sarbanes-Oxley focuses on a subset of the COSO framework, considering internal controls over financial statement preparation and disclosures.

Now that organizations have a process and staff in place to document and evaluate internal controls, it’s time to put them to use enterprisewide.

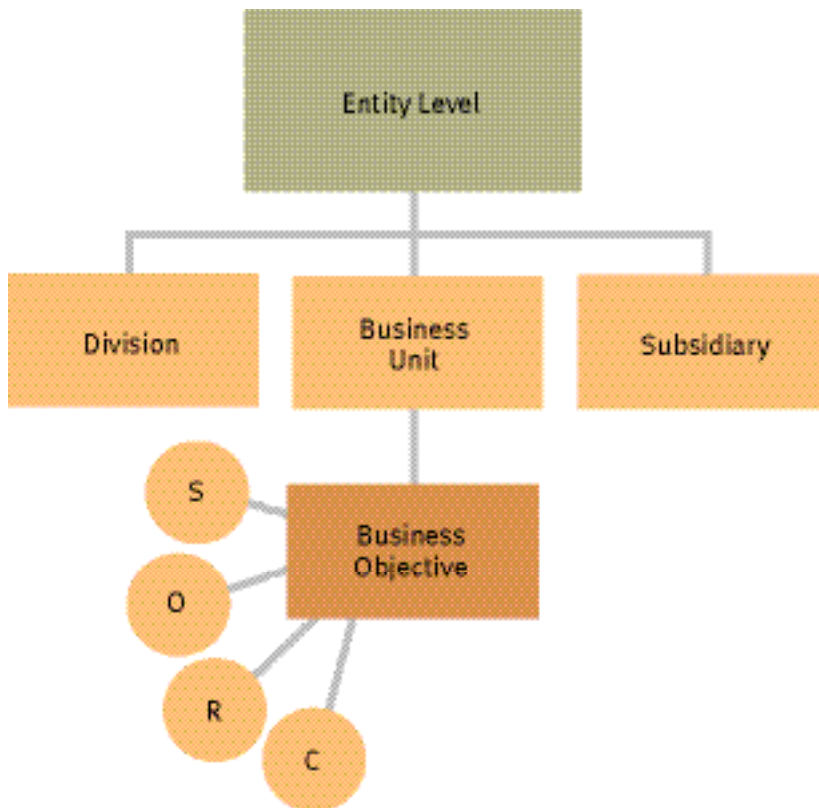
ENTERPRISE RISK MANAGEMENT

The newly released COSO *Enterprise Risk Management–Integrated Framework* builds on the IC-IF and provides the structure for taking the work done for Sarbanes-Oxley and implementing it enterprisewide. It emphasizes the importance of identifying and managing risks across the enterprise. The “COSO ERM Cube,” which appears on this page, comprises four vertical objective categories: strategic, operations, reporting, and compliance. Its eight horizontal components consist of: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. Whereas many organizations perform isolated risk management activities within silos, COSO’s vision is that risks should be aggregated and viewed from the top as an overall portfolio of risk.

The board of directors has overall responsibility for risk management, which is delegated operationally to all levels of management across the organizational structure. Ultimately, however, ERM’s success is dependent upon everyone through the alignment of people, strategy, objectives, resources, needs, and priorities in the context of the entity’s internal environment.

A COSO ERM solution begins by identifying the business units, divisions, and subsidiaries at the enterprise or entity level

Entity Level Breakdown



of the organization (see “Entity Level Breakdown” on page 68). The entity level and its organizational units are depicted by the third dimension of the ERM cube.

Next, the enterprise’s CEO identifies objectives and strategic alternatives — his or her vision for the success of the enterprise — and categorizes them as strategic, operations, reporting, and compliance (SORC in the “Entity Level Breakdown” chart on page 68). Each of the heads of the business units, divisions, and subsidiaries also identify their objectives, which must integrate with the enterprise objectives.

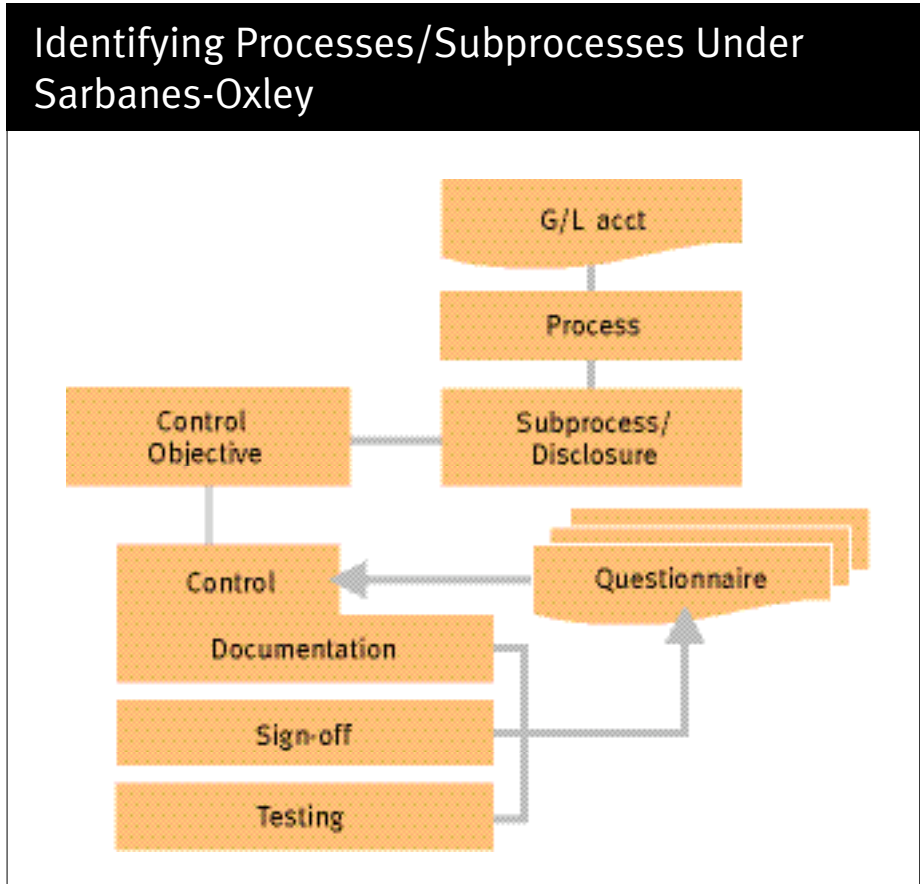
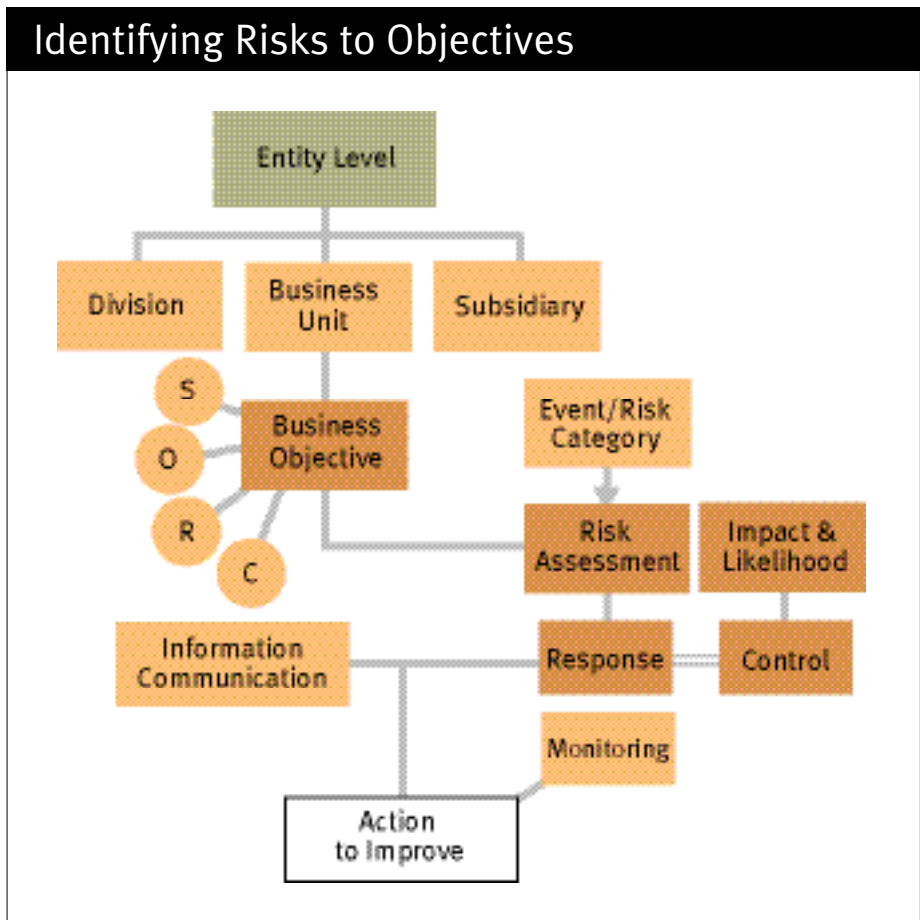
Once objectives have been identified, the next exercise is to identify the risks that will prevent management from achieving its objectives (see “Identifying Risks to Objectives” on this page). For example, an objective may be to source new products from China. The risks associated with that objective might include integrity of supplier, government issues, quality of work, acceptance by customers, and delivery times.

Management also identifies events that could influence the risk, either positively or negatively, and the probability of them occurring. Events — and all of risk management — are a dynamic process. For example, will the threat of the SARS virus affect the Hong Kong operation? That’s a dynamic risk that can be addressed. The Sept. 11 disaster in New York was something that could not have been foreseen. Thus, the risk could not have been calculated.

In addition to identifying risks, management assesses the impact the risk will have on the organization and the likelihood the risk will occur. The combination of impact and likelihood is a ranking of risks, and it behooves the organization to address those risks with high impact and likelihood.

Once the risks have been identified and ranked, the controls needed to mitigate them are chosen. The strategy a company adopts to manage risks varies according to the organization’s risk-taking preferences — or risk appetite. Risk management experts often summarize the options as treat, terminate, transfer, or take (or tolerate) — the four T’s.

Treating a risk means taking direct action to reduce either its impact or its likelihood of occurrence. Often, the treatment is internal control. In the China example, one means of mitigating the customer acceptance risk might



be via a marketing campaign — not something most people would think of immediately as a control.

To terminate a risk is to walk away from it. A company with a low risk appetite, faced with the risks of sourcing products from China, may decide to source products elsewhere.

Risks may also be transferred to others through insurance or contracts, often with outsourced service suppliers. However, the primary risk often remains with its original owner. If the right goods don't reach a retail store on time and in good condition, there may be a penalty clause that can be invoked against the logistics supplier, but it is still the retailer who loses sales and customer good will.

Finally, there are some risks that the organization must accept, tolerate, or take. Companies with high risk appetites and

good risk management processes often reap the rewards of higher profits.

Once risk response strategies have been selected, management undertakes control and other risk response activities. Management tests to ensure that the design of the controls and other response activities is appropriate and that the controls and response activities themselves work at each business level.

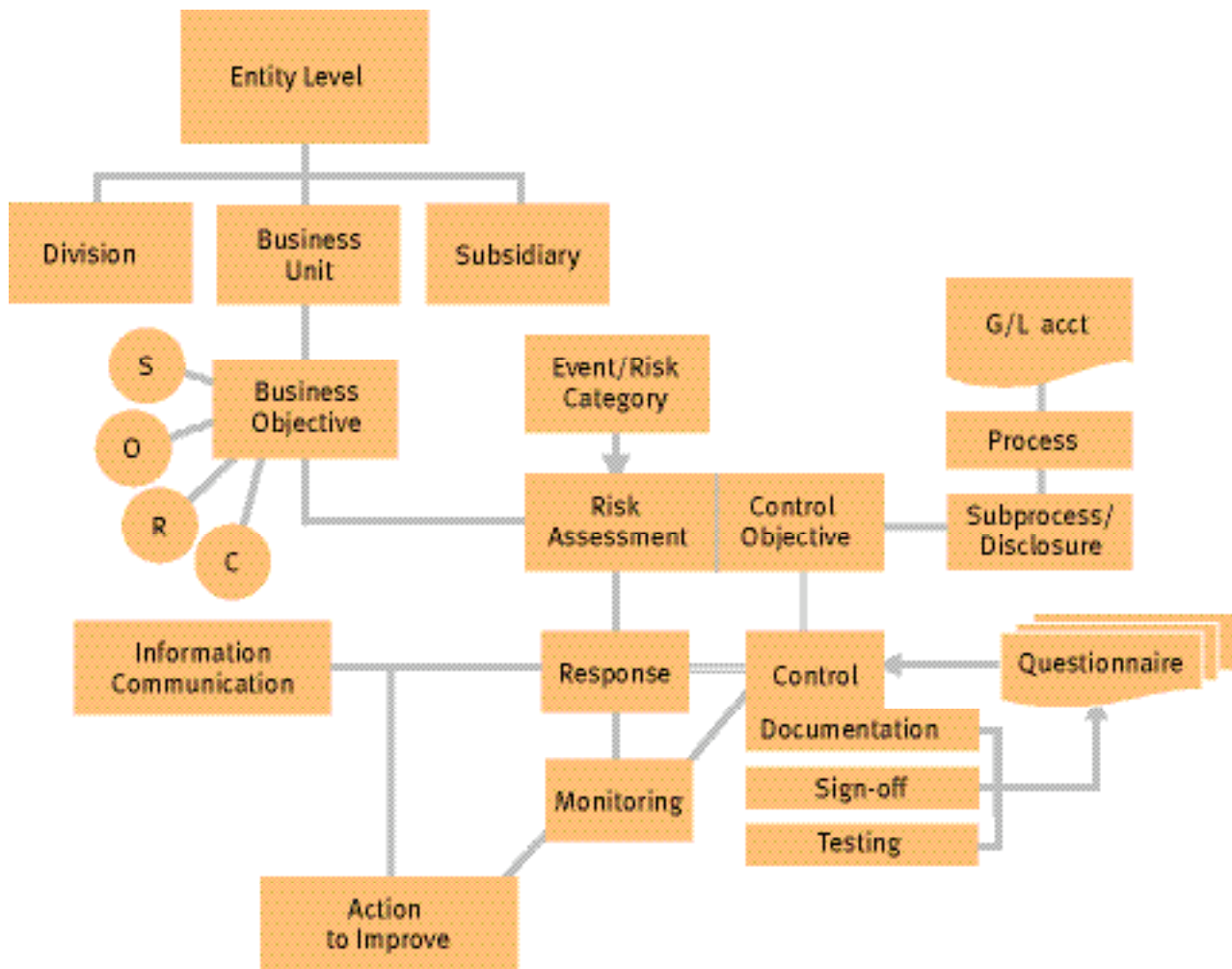
Note that the process just described is no different from the Sarbanes-Oxley exercise companies have been conducting, except here management is analyzing operations rather than financial risks. When addressing Sarbanes-Oxley, an organization starts with the financial statements from which its processes and subprocesses are identified (see "Identifying Processes/Subprocesses under Sarbanes-Oxley," page 69). Next, the company

identifies the control objectives to mitigate risks associated with the processes. Management then documents the controls, obtains a sign-off on the controls, and tests them to be sure they are in place and functioning adequately. Finally, management implements assurance activities that may include a control self-assessment system and questionnaires to follow up on the controls and testing process. Sarbanes-Oxley is actually a subset of COSO ERM (see "COSO + Sarbanes-Oxley = Total ERM" on this page).

INTERNAL AUDITING'S ROLE

Managers own risks, and it is their responsibility to control them. Internal auditing provides objective assurance to the board on the effectiveness of ERM. Internal auditors may be asked to provide advice, and more, on risk management, providing:

COSO + Sarbanes-Oxley = Total ERM



Inherent Risks					
GROSS/INHERENT RISK RATE					
Critical	2	0	0	0	2
Significant	0	5	1	3	2
Moderate	1	4	5	4	2
Low	2	4	2	3	1
Insignificant	2	2	1	0	1
	Remote	Unlikely	Likely	Probable	Highly Probable

Residual Risks					
NET/RESIDUAL RISK RATE					
Critical	0	0	0	1	1
Significant	3	2	4	0	0
Moderate	1	3	4	0	1
Low	2	3	4	2	0
Insignificant	11	4	1	1	0
	Remote	Unlikely	Likely	Probable	Highly Probable

- It doesn't compromise the auditors' independence and objectivity.
- The resources required don't hinder them from achieving their main objective of assurance.
- Managers don't come to regard the auditors as the risk owner. Internal auditing is providing assurance to management, not the other way around.

ERM is a process in itself that must be included in governance objectives. Internal auditing focuses on management's approach to risk management — understanding management's strategic, operational, and value objectives; identifying and evaluating the key business risks that are barriers to achieving those objectives; understanding management's tolerance relative to risk occurrence; determining the risk management activities deployed to manage the risks to an acceptable level; and assessing the effectiveness of those risk management activities. It is the auditor's job to assure the audit committee that the risk management process is working.

DEVELOPING THE AUDIT PLAN

The objective of risk management auditing is to minimize the risk of audit failure by selecting the appropriate processes or areas to audit. Typically, companies use a matrix to analyze a risk's likelihood and

impact. The company first considers gross or inherent risks, those that will prevent it from achieving its objectives (see "Inherent Risks" on this page), and implements response strategies to mitigate those risks. The company then considers the net or residual risk. In the "Residual Risks" chart that appears on this page, each element is assigned a value: 1 is remote and insignificant; 25 is critical and highly probable. The critical question is how have the controls mitigated the gross risk to reduce the net risk?

In the "Analyzing Risk and Controls," graph that appears on this page, management has identified risks as high or low, and controls as weak or strong. Internal auditing spends its resources auditing those processes with high risk and strong controls to ascertain that the inherent risks are, in fact, mitigated by risk response strategies and controls. For those processes identified with a high risk and weak controls, internal auditing focuses on whether management has an adequate action plan in place to improve the controls. The real area of concern is with low risks. At first glance, one would think these areas should be ignored. Rather, internal auditing should review management's evaluation of impact and likelihood of risks or events occurring.

Internal auditing establishes a combination of substantive and compliance tests to ensure that risk management activities are designed effectively. They then test the processes to see that the risk response, strategies, and controls are in place and mitigating the risks, and that the eight components of COSO ERM are satisfied.

ONLY THE BEGINNING

Although Sarbanes-Oxley may have caused much consternation, it also generated benefits to stakeholders, including:

- Executives are beginning to see risk management as a strategic activity.
- Risk standards can ensure uniform risk assessment across the organization.
- Risk management values have become culturally ingrained.
- Risk considerations have become part of everyday business decision-making.
- Resources are likely to be allocated to the risks that are most important.
- Decision-making is based on full knowledge of risks and controls.
- Internal and external reporting of risk and control information is enhanced.
- Responsiveness to change has increased.
- Communication and knowledge sharing are improved.

According to various studies, an ERM solution would normally take two to three years to implement. However, because much of this work has been done in the Sarbanes-Oxley exercise, in particular establishing a COSO framework, the time to implement ERM is now much reduced.

The cost of complying with Sarbanes-Oxley can be anywhere from \$1 million to \$25 million, depending on the size and complexity of the organization. And estimates show that companies will spend 50 percent of the implementation cost for ongoing maintenance. So why not make part of that expenditure include adopting a total ERM solution? Going beyond the single COSO reporting category and including strategic, operations, and compliance, enables companies to manage risk interdependencies — and thereby capitalize by being in total control.

To comment on this article, contact the authors at gmatyjewicz@theiia.org.

Analyzing Risk and Controls			
Risk	High	1	2
	Low	4	3
		Weak	Strong
		Controls	