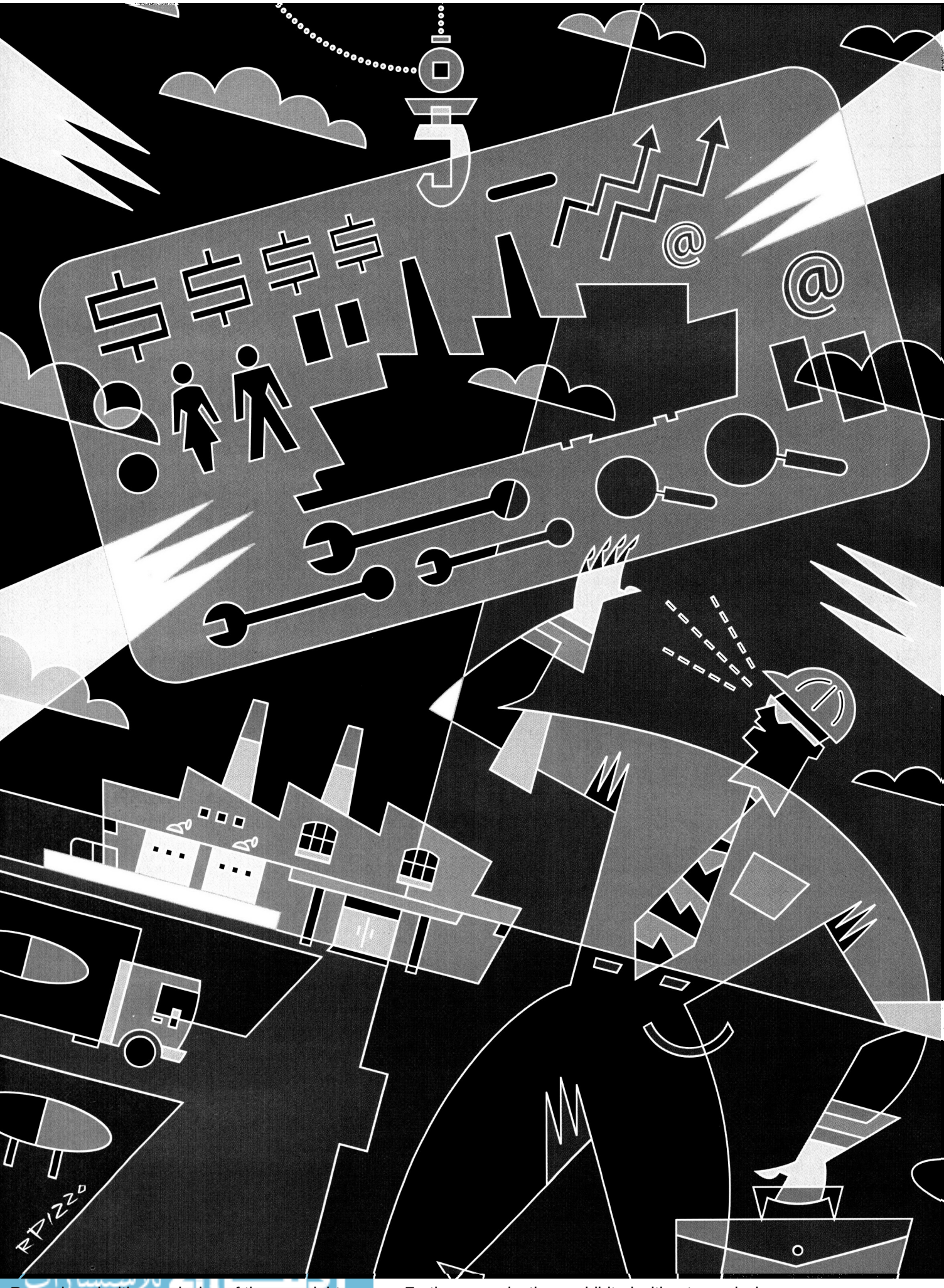
Make Risk Management and Internal Control Work for YOU

Schwartz, R Malcolm

Strategic Finance; Dec 2006; 88, 6; ProQuest Central
pg. 34



Make **Risk Management** and **Internal Control** Work for **YOU**

By tailoring an integrated, business-process-based template solution, small companies can address risks and controls in a cost-effective manner, whether or not SOX compliance is mandated.

BY R MALCOLM SCHWARTZ, CMA, CMC

Smaller companies are avoiding risk management and internal control efforts because they hope that the Securities & Exchange Commission (SEC) won't require them to comply with the Sarbanes-Oxley Act (SOX). They are frightened by reports of the high cost of compliance activities, such as more than 2% of revenue reported for a $25-million revenue company.

But the reality is that SOX compliance doesn't have to cost a lot, as I'll demonstrate in the following guidance on how to do risk and controls management at a reasonable cost. This guidance is important to smaller companies, which generally have limited skills, experience, and tools for operating cost-effective internal control and risk management programs. A second reality is that risk and controls management is good for you and can provide substantial benefits whether SOX compliance is required or not. So, don't make controls and risk management dependent on whether you are obligated to comply.

For its cost, which can be reasonable, good risk and controls management has a pretty direct correlation with good performance. For example, several years ago, before SOX, a consumer products company used the *Internal Control—Integrated Framework* from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) to assess internal control in its five business units (remember that internal control in the COSO Framework begins with business-centric risk assessment). It found a direct correlation between control and performance. The poorest-performing unit was on the verge of

ILLUSTRATION: ROBERT PIZZO/WWW.ROBERTPIZZO.COM

being out of control and was sold shortly thereafter, primarily to cleanse the corporate portfolio of a major business risk.

This anecdote, which is supported by research, illustrates the relationship between control and performance. For example, a study conducted at the London School of Economics in 2005 by McKinsey and the Center for Economic Performance indicates that managers and their competencies and motivations—basic principles of good risk and controls management—are more important to how a company performs than other structural factors. In other words, mediocre control goes hand in hand with mediocre corporate results. The research notes that, in studying 18 management practices:

◆ One company used monitoring (one of the five components of control in the COSO Framework) to spur action only when output dipped. It then discontinued the monitoring when output rose, so there was no way to track performance with business objectives. This is consistent with Level 1 control, as defined in one of the tools I developed to apply the original COSO Framework effectively. The tool contains questions to ask about the five components in the COSO Framework and then provides four levels of answers to each question. Level 1 is applied to answers that indicate that the organization would only know it was out of control if it were told so by an outside party, such as a regulator or a reporter.

◆ A second company monitored performance indicators continually but didn't share this information with the operating personnel, depriving them and the company of improvement efforts. This is Level 2 control, which works adequately in periods of stability (and most organizations don't have the option of being in periods of stability).

◆ A third company set up display screens to show personnel where their performance ranked along with daily targets and other goals. Managers provided a monthly overview and summary, met with operating personnel every morning to discuss the previous day's performance and the current day's agenda, and used lunch breaks as opportunities for feedback on performance, achievements, and improvement opportunities This is beyond Level 3 control (control in the face of change), and verges on Level 4 control (control capable of dealing with the unusual situations called "acts of God").

The research also indicates a statistically supportable correlation in performance among these companies. There are several lessons here: First, good people enable good performance. Second, sound management techniques incorporating management of risk and controls provide a setting for good people to perform better. Third, control as envisioned in the principles of the COSO Framework—beginning with a control environment of competent people, well-designed policies and procedures, effective communications, reinforced human resources policies, and risk assessment—is built into those techniques. Fourth, the techniques provide a focus for goals, for performance in the context of current practices, and for improving current practices. The result is a premium on working smarter, not working harder—and working smarter includes managing risks and controls cost effectively.

Whatever the SEC decides, make internal control and risk management work for you first. Then make it work for your auditors second, if at all.

THE RIGHT APPROACH

Now that we know risk and controls management is good for you, the next question is: Can it be less painful than is generally being reported? The answer is "yes." I'll show you a low-cost, high-value method that is worth implementing whether compliance is mandated or not. This "better way" is based on using a generic, integrated, business-process-based template and involves following a step-by-step implementation approach. To help illustrate the method, I'll also discuss a case study where a small public company used the template and approach. By the way, the cost of this application was in the area of several person-months of internal effort, a similar amount of some incremental consulting, and about $25,000 in software costs, which is nowhere near the millions of dollars and person-hours that are being reported for risk and controls management approaches. Basically, the steps for the right approach are:

1. Start with an integrated, business-process-based template solution. Tailor the business processes being analyzed, the activity components of those processes, and the activity characteristics to your business and circumstances.

2. Tailor the risk assessments in the template to identify the activities that involve enough risk that they need controls. These controls take the form of control activities.

3. Tailor the control activities and roles in the template to fit your needs to mitigate risk.

4. Finish tailoring the template to relate to financial statements in order to complete the integrated documentation and the focus on financial reporting objectives.

5. Tailor the monitoring activities in the template to use them to oversee and confirm your control activities;

Table 1: The Generic Template—Processes, Activities, and Attributes: Overall and for "Process Accounts Payable"

PROCESS HIERARCHY (SELECTIVE)	ATTRIBUTES										
	ACTIVITY TYPE	ASSERTION	AUTOMATION PROFILE	CONTROL HIERARCHY	CONTROL LEVEL	CONTROL TYPE	CONTROL KCI	COSO MAPPING	FREQUENCY PROFILE	RISK MEASURE	RISK TYPE
Run the business											
Manage finance—control, treasury, tax, and audit											
Record and present plans											
Record, monitor, and present results											
Process accounts payable											
Receive copy of receiving report (RR)	O		S	T				CA	O	LL	I
Align RR with purchase order (PO), and initial RR	O		S	T	O	P	AC	CA	O	LL	I
Receive Authorization to Pay (ATP)	O		M	T				CA	O	LL	I
Align ATP with PO, and initial ATP	O		S	T	O	P	AC	CA	O	LL	I
Confirm RR/ATP is valid for role and receipt	O		S	T	O	D	C	CA	O	LL	I
Calculate and post balance to receive on PO	O		S	T	O	P	AS	CA	O	LL	I
Receive vendor invoice, and post to Payables Controls Log (PCL)	O		S	T		P	ACS	CA	O	LL	I
Confirm vendor invoice to RR/ATP and PO, and post to PCL	O		S	T		P	AS	CA	O	LL	I
File copy of PO	O		M	T				CA	O	LL	I
Prepare voucher, attach vendor invoice, and post to PCL	O		S	T		P	ACST	CA	O	LM	I
Approve voucher, and post to PCL	C		S	T	O	D	ACST	CA	O	LL	R
Enter voucher to general ledger, and post to PCL	O		S	T		P	AST	CA	D	ML	I
Approve general ledger posting, and post to PCL	C	EO	S	B	O	D	ACST	CA	D	LL	R
Certify accounts payable process	M		M	B	O	P	ACST	M	D	LL	R
Process accounts receivable											
Process funds											
Process fixed assets and leaseholds											
Process benefits and retiree information											
Process payroll											
Process tax compliance											
Process standard costs											
Analyze and reconcile											
Provide financial and management reporting											
Maintain accounting policy, schedules, and procedures											
Safeguard assets											
Manage the enterprise											
Manage external relations											
Provide administrative services											
Manage information systems											
Manage risks											
Manage legal affairs											
Plan											
Manage human resources											
Develop and apply technology											
Procure goods and services											
Conduct inbound activities											
Conduct operations											
Conduct outbound activities											
Conduct marketing and sales activities											
Provide customer services											

LEGEND

Activity Type: O(perational), C(ontrol), M(onitoring)

Assertion: E(xistence) O(ccurence)

Automation Profile: S(emi-automated), M(anual), A(utomated)

Control Hierarchy: T(ransaction), B(usiness unit), C(orporate)

Control Level: K(ey), O(ther)

Control Type: P(reventive), D(etective)

Control KCI: A(ccurate), S(ummary, or complete), C(ompliant), T(imely)

COSO Map: C(ontrol) E(nvironment), R(isk) A(ssessment), C(ontrol) A(ctivity), I(nformation) C(ommunication), M(onitoring)

Frequency: O(ccurrence), D(aily), W(eekly), M(onthly), Q(uarterly)

Risk Measure: L(ow), M(oderate), H(igh), for magnitude and duration, respectively

Risk Type: I(nherent), R(esidual)

then use key control indicators to tailor the separate evaluations—the testing—of the design of control activities and of the performance of control and monitoring.

Using this approach saves time and money because: (1) a solution doesn't need to be created outright, only tailored from an existing template; (2) it focuses on documenting only those activities that need controls; (3) only one set of integrated documentation—which is easy to create and maintain—is needed; and (4) testing is reduced to the specific needs of overseeing the built-in monitoring.

Now let's take a closer look at the five steps.

Step 1: Start with an Integrated, Business-Process-Based Template Solution

The template solution lets you take advantage of a best- or accepted-practices generic model and make it specific to your business. With it, you have in place the processes, the components of processes (the activities) and their inputs and outputs (results), and the characteristics (the attributes) that let you manage the activities and establish controls and risk management. To base compliance on processes, you must be clear about what a process is and that the outputs of each process and of each of its activities have specific values associated with them. These values, called key control indicators (KCIs), can include accuracy, timeliness, completeness, and compliance (with both internal policies and external laws and regulations). They vary depending on what is appropriate to the activity.

This approach enables the integration of control with fraud protection. Not treating fraud protection as a separate subject helps reduce compliance costs even more.

The template used to illustrate this approach is fully developed and is contained in Table 1. To show you its features, I'll use an example from it that will include an illustrative process and its activities and associated roles; linkages to financial statement accounts; and risk, business, and control attributes—including risk profile, level of automation, cost, form and frequency of monitoring and testing, needs for improvement or remediation, and such control features as hierarchy, level, type, and so forth.

The example is "Process accounts payable." I selected this process because it involves a tailored solution to the generic template that shows how to deal with an area of major risk regarding accurate financial statements. It also involves transaction and management processes and fraud detection, illustrating how these different types of processes can be integrated.

The template integrates transaction, management, and governance processes, thus eliminating the costs and risks of developing, applying, and maintaining separate spreadsheets and checklists. It also integrates COSO, COBIT (Control Objectives for Information and related Technology), and basic transaction processes.

When this template was applied to a smaller registrant, it led to much lower compliance costs. The benefits of this approach were realized when the template was applied to a smaller, public, professional services firm.

Project Overview. The project began after some discussion between the CFO and the external audit team, who knew the business well enough to agree with the CFO's assessment of top-down risk. They decided that from the standpoint of financial reporting they would look at major compliance risks in the areas of payroll, accounts payable, accounts receivable, the period closing, and external financial reporting. Following a review with the Audit Committee and its concurrence, the CFO expanded that focus to include management processes related to the COSO Framework and IT controls. That led to accepting the generic template "as is" for all other business processes, with the possibility of making refinements at some later date, and focusing the project charter and any tailoring activities on those four transaction process areas and the two management process areas.

The CFO met with his team about the work to follow. He then added to his team a full-time management consultant who was knowledgeable about the targeted processes, as well as about business process documentation and analysis in general; a part-time systems consultant who was knowledgeable about the template and the software being used by the template; and a part-time senior consultant who knew internal controls and risk management, had applied these subjects to SOX compliance, and who would provide quality assurance on the consulting team.

The CFO and his team spent a day in training about the management of internal controls and risk and on the template and the software it used. Then he and the relevant members of his team met with the management consultant to review the generic template for each of the targeted process areas and tailor it to their approach. Each of the meetings ran between one and one-a-half hours. The consultant was able to do much of the tailoring during the course of each meeting, and he also sought technical guidance from the systems consultant and reviewed the tailored version with the senior consultant after the meeting. Then he either tailored the generic

Table 2: The Tailored Template for "Process Acccounts Payable"

Process accounts payable (tailored approach shown in green and remediation shown in orange)

INPUTS TO ACTIVITIES	ACTIVITIES	OUTPUTS FROM ACTIVITIES
RR, A/P copy, prepared	Receive copy of receiving report (RR)	Receiving report, A/P copy, received
RR, A/P copy, received (1)	Align RR with purchase order (PO), and initial RR	RR, A/P copy, initialed
PO, A/P copy (1)		
ATP, A/P copy, prepared	Receive Authorization to Pay (ATP)	ATP, A/P copy, received
Payroll tax payments, authorized		
Tax payment, authorized		
Benefits payment, authorized		
Pension payment, authorized		
ATP, A/P copy, received	Align ATP with PO, and initial ATP	ATP, A/P copy, initialed
PO, A/P copy (3)		
RR, A/P copy, received (2)		
Authorization table, updated, approved	Confirm RR/ATP is valid for role and receipt	RR, A/P copy, validated for role and receipt
PO, A/P copy (2)		ATP, A/P copy, validated for role and receipt
ATP, A/P copy, initialed		
RR, A/P copy, initialed		
PO, A/P copy (4)	Calculate and post balance to receive on PO	PO, A/P copy, noted for balance open
Vendor invoice, received (external)	Receive vendor invoice, and post to Payables Controls Log (PCL)	Vendor invoice, pending approval PCL, posted with vendor invoice
Vendor list, authorized, current		
PCL form		
PCL, posted with vendor invoice	Confirm vendor invoice to RR/ATP and PO, and post to PCL	Vendor invoice, confirmed
ATP, A/P copy, validated for role and receipt		PCL, posted with RR-ATP/PO match
RR, A/P copy, validated for role and receipt		
PO, A/P copy, noted for balance open	File copy of PO	
A/P voucher form, current	Prepare voucher, attach vendor invoice, and post to PCL	A/P voucher, prepared, with attached vendor invoice
PCL, posted with RR-ATP/PO match		PCL, with A/P voucher KCI information
Vendor invoice, confirmed		
A/P voucher, prepared, with attached vendor invoice	Approve voucher, and post to PCL	A/P voucher, approved, transmitted
PCL, with A/P voucher KCI information		PCL, posted with approved A/P voucher KCIs
General ledger (GL), current, approved	Enter voucher to general ledger, and post to PCL	A/P voucher, entered on JE to GL
Journal entry (JE) form, current, approved		PCL, posted with GL KCI information
A/P voucher, approved, transmitted		
PCL, posted with approved A/P voucher KCIs		
PCL, posted with GL KCI information	Approve general ledger posting, and post to PCL	PCL, completed
PCL, completed	Certify accounts payable process	A/P process certification report
Policy and procedure, A/P, current		
A/P processor, current appraisal, approved		
A/P processor, current development plan, approved		
Controller, current appraisal, approved		
Controller, current development plan, approved		

template to reflect the wording of the process and its activities as they are performed by the CFO and his team or modified the process to follow recommended approaches that would address any issues of control and risk management. For example, because the company had a small staff, some problems arose with segregation of duties, so the consultant added more reviews by the audit committee to the tailored template.

Each process team then had a second meeting of about the same length to review the results of their first meeting, to see and accept or reject what the consultant had done and recommended, and to make any further refinements to the documentation. If any remediation or modification were necessary, the CFO reviewed relevant policies, procedures, position descriptions, systems documentation, and so on, to update and align them. He also

kept the audit committee informed and made the process and risk-and-control documentation available to committee members.

After reviewing the accounts payable process, the CFO and his team decided to narrow the scope of the generic model to focus on their primary concern, namely the accuracy and relevancy of—and risk of fraud in—time and expense reports submitted by staff and by contractors. They considered other areas of the payables process to be either small in monetary scope or reasonably routine in practice and hence not contributing to risk in financial reporting. Because the process was automated, the team relied on the system-generated reports for reviews of controls performance. This tailoring is shown in Table 2.

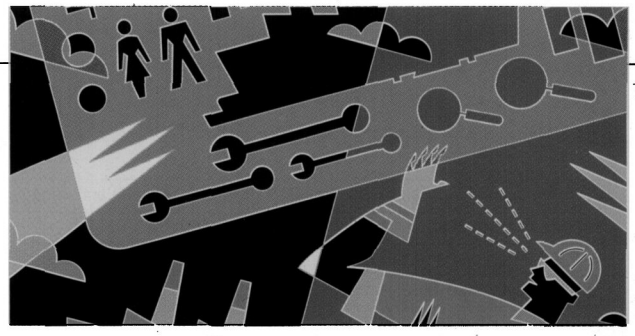
At the same time, the consulting team recommended some improvements in documentation—largely in the areas of policy and procedures—an approved vendor list, and the use of performance appraisals and development plans as integral to the process certification. All of these areas were addressed and didn't take much time to fix.

If you were to follow this CFO's approach, the key actions are to: (1) train knowledgeable persons on this approach, then meet to cover each process end-to-end from the viewpoints of designing, performing, and monitoring the process; (2) review the template, have the group focus on relevant risks in relevant processes, and modify those processes and their activities to fit the business; (3) update the template by completing any revisions off-line; and (4) schedule a second meeting to accept the tailored model. During these steps, also use the tailoring exercise to identify improvement opportunities and needs and to set up the improvement program so that remediation and continual improvements are built into management processes.

Step 2: Tailor the Risk Assessment in the Template

In any process, some activities have a high enough level of uncertainty in their outputs to cause a moderate or greater risk to the quality—the accuracy, completeness, compliance, and/or timeliness—of the outputs and of the overall process. These are the output risks that are inherent to the process. The way to mitigate these inherent risks is to build control activities into the process that, if well designed and in turn well performed, will reduce the inherent risk in the process to an acceptable residual risk.

By focusing on the risks in the activity components of the process, managers can reduce documentation to that for the outputs of those activities with inherent risk at



levels of concern and for the control activities themselves. In practice, this step has led to reducing the amount of documentation by factors of four or more. The activity-level characteristics in the template allow you to look at the costs of controls related to the benefit of mitigating the risk and then to tailor the template for your purposes.

In our accounts payable illustration, the CFO had used risk assessment broadly to identify processes of concern. In the second, sign-off meeting with each process team for the previous step, he reviewed the risk characteristics in the generic template for each of the activities in the process being reviewed and resolved. Then the team tailored the activity-level risk assessments to its business. For the accounts payable process, as shown in Table 3, the team assigned higher risk ratings than in the generic template to those activities dealing with expense reports and with contractors' invoices because these activities were deemed to be riskier for a professional services business than for a general business.

The team also checked the linkages of these activities with specific financial accounts in the generic template, and it reviewed all other linkages in the generic template to those accounts to check whether other processes and their activities might be sources of financial reporting risk. Finally, they were satisfied that they had identified the important, and few, risks and associated activities. The management consultant finished tailoring the template off-line after each team meeting.

To follow the approach used in the case study: (1) Review the risks by activity, and tailor them to your business; and (2) check that the activities and their risks provide the protection for key financial statement exposures. By following this approach at the activity level, documentation—and, hence, cost—can be reduced substantially.

Step 3: Tailor the Control Activities in the Template

Once activities with key risks have been identified and the generic template has been tailored to your business, the next step is to confirm that the control activities are designed and placed where they should be. When the uncertainty in the process output reaches a level of con-

Table 3: Tailored Activities and Attributes

	TAILORED ATTRIBUTES												TAILORED RESOURCES	
TAILORED ACTIVITIES	ACTIVITY TYPE	ASSERTION	AUTOMATION PROFILE	CONTROL HIERARCHY	CONTROL LEVEL	CONTROL TYPE	CONTROL KCI	COSO MAPPING	FREQUENCY PROFILE	RISK MEASURE	RISK TYPE	ROLE	SYSTEM	FINANCIAL STATEMENT ACCOUNTS
Receive copy of receiving report (RR)	O		A	T					O	LL	I	AP	AP	
Receive Authorization to Pay (ATP)	O		M	T					O	LL	I	AP		
Confirm RR/ATP is valid for role and receipt	O		S	T	O	D	C		O	LL	I	AP	AP	
Confirm vendor invoice to RR/ATP and PO, and apply codes	O		S	T		P	AS		O	LL	I	AP	AP	
Enter coded invoice to system	O		A	T		P	AST		O	MM	I	AP	AP, GL	AP, various E
Approve general ledger posting	C	EO	S	B	K	D	ACST	CA	D	LL	R	C	AP, GL	AP, various E
Certify accounts payable process	M		M	B	O	P	ACST	M	D	LL	R	CFO	AP, GL	

LEGEND FOR RESOURCES

Role: AP(clerk), C(ontroller), CFO

System: AP(system), GL(system)

Financial statement accounts: AP, E(xpense)

cern that could lead to a material weakness, this inherent risk is addressed by the control activity to bring the design risk to an acceptable level of residual risk. Removing the control activity or performing it poorly would return the process to an unacceptable level of inherent risk. Performing these well-designed control activities well, on the other hand, results in an acceptable level of residual risk. In effect, control activities reduce the variability of the basic operations activities in a process.

The uncertainty, or variability, is identified in the generic template along two dimensions of exposure—magnitude and duration. The template deals with these dimensions qualitatively, recording exposure as high, medium, or low, but some companies prefer that these dimensions be quantified or even monetized. This process can be accomplished during the tailoring of the template.

Furthermore, the measures of variability in an activity correlate to the statements of assertion, which are used by the PCAOB and auditors to define assertions that the CFO and his/her team make in regard to its accuracy, propriety, timeliness, and so forth, about their work and work products. They refer to the features of accounting and reporting. Therefore, instead of simply asserting the assertions or mapping them to controls, you can put monitoring activities in place that track the dimensions of controls—using key control indicators (KCIs). By doing this you will be in a position to assess control performance as well as to relate to the statements of assertion.

During the second, sign-off meeting for each process, the CFO had the team review the control activities in the generic template, particularly regarding their design, placement, and outputs. For the accounts payable process, the team felt that the control activities as designed in the generic template were for a less automated operation with higher volumes, so they simplified and automated the Payables Controls Log while retaining the use of key control indicators for continual monitoring (or "ongoing monitoring," as described in the COSO Framework), shown in Table 3.

In summary, to use the generic template and to follow the approach in the case study: (1) Review the control activities in the template in relation to the tailored risk profile, and tailor the control activities to conform; and (2) finish tailoring the template off-line. To be cost effective, the bulk of the documentation should be of the control activities.

Step 4: Finish Tailoring the Template

It's important to relate activities and risks to resources. In the generic template, these resources include roles, software, other tools, and financial statement accounts. Roles are important for separation of duties. Software and other tools, such as forms and control logs, are important as enablers. Linkages to financial statement accounts are important for compliance. But beginning with an account tends to cause people to focus on the size of the account, with an emphasis on coverage of a sufficient portion of the financial statements, as opposed to the risk in not having an accurate portrayal of the financial statements. A smaller account balance might be an area for major misstatement, whereas a larger account balance might cause very little exposure to misstatements. The primary reason

for this is that the larger accounts tend to have reasonable, well-controlled systems and procedures, whereas many smaller accounts are based much more on judgment and hence are subject to being played with; an example is the large account for accounts receivable and the smaller associated account for the reserve on receivables. Beginning with an account also tends to lead to documenting everything that affects that account once that account is deemed to be large. So it makes sense to isolate the risky activities and then to focus on controlling them.

The generic template provides a view by activity on these three types of resources, which can be tailored. This view shows how financial statement accounts and roles are related to activities. The roles, in turn, relate to position descriptions, which are linked with appraisals and with development plans. This is consistent with the COSO Framework.

For the accounts payable process, the generic template links these as part of the "horizontal" certification of the process, the sign-off by the CFO. In the case study, after the second, sign-off meeting, the CFO decided to follow this approach because it supported segregation of duties and provided the audit committee a written summary of the performance of this key process and its key controls. Roles and accounts are shown in Table 3.

In summary, although every process team might meet regarding each of these steps, the CFO in the case study combined the steps because they had distinctive content but didn't merit separate meetings. The main point of this step, whether done separately or not, is to confirm the placement and tailoring of the control activities and to confirm the appropriate relationship to the resources of roles, tools, and accounts. Note that, as was done in the case study, you can limit participants for this effort to financial, control, and audit people, who can confirm and tailor the design of the activities and risks to the financial statements. Using the template to describe roles, tools, and resources and then tailoring this information to your situation enables much of the documentation to be in place and all of the documentation to be integrated. Both of these features add to the cost effectiveness of the approach.

Step 5: Tailor the Monitoring Activities in the Template

Use ongoing monitoring from the control and compliance standpoint to stress accountability of the activity and process owners so that control is understood to be basic to the work activities. Use ongoing monitoring from the business standpoint to assess control so that control—compared to targets and to committed levels—is always understood and corrections are made continually.

Only use separate evaluations, then, to assess the performance of your ongoing monitoring, not to assess control. This strategy reduces the cost of testing while enabling monitoring to have more impact.

Also use ongoing monitoring as the basis for certifications and to define the scope and focus of separate evaluations. Certification functions somewhat as a control step, as well as a means to manage the process, and it also is the basis for SOX Section 302 compliance—the certification by the CFO and the CEO in regard to effective control over financial reporting and disclosure—for each particular process.

In the generic template, certification is a final activity in each process and, in many cases, in the subprocess where the process is complex. In turn, these certifications are assembled as inputs to the overall compliance review as well as to reviews that shape separate evaluations and external audit scope and activities. These monitoring and certification activities are shown in summary in Tables 2 and 3.

In the case study, the CFO put the ongoing monitoring in place using KCIs as each process and its risks and controls were tailored to the business. He then reviewed the results from the ongoing monitoring with the external auditor team. This met the goal of separate evaluations as performed by the CFO and the internal audit committee and then independently assessed by the external auditor.

In summary, the CFO was able to apply and tailor the template at a reasonable cost and with a reasonable level of activity. And he and his team built in some controls that made the business work better; for example, billings to clients were easier to assemble and were submitted in a more timely fashion.

As you can see, there *is* hope for a cost-effective solution for Sarbanes-Oxley compliance. And there's hope that addressing business risks and controls in this way will provide business benefits whether or not compliance with SOX is mandated. ■

R Malcolm Schwartz, CMA, CMC, is chief operating officer of CRS Associates, LLC, a consulting company with one focus on integrating operations improvement with Sarbanes-Oxley compliance. While at Coopers & Lybrand, he was one of the principal authors of the 1992 COSO report, Internal Control—Integrated Framework, *and he recently served on the COSO Task Force developing simplified guidelines for smaller companies. You can reach him at (908) 273-6967 or malcolm@crsassociatesllc.com.*