A Higher Level of Governance—Monitoring IT Internal Controls

In the past few years, senior management’s interest in good internal controls has increased. Surveys in recent financial magazines show that many chief financial officers (CFOs) would like to have internal control monitoring programs in their enterprises, but do not know where to start to develop a program.1, 2

WHAT HAS CHANGED

Many public and private agencies are requiring verification that internal controls are in place and operating effectively—at all times. In the US, the Sarbanes-Oxley Act of 2002 mandates effective controls for financial reporting. Many companies, particularly in Europe, require certifications that show compliance with various International Organization for Standardization (ISO) process standards. Credit card companies are requiring compliance with the Payment Card Industry Data Security Standard (PCI DSS). Internationally, privacy laws are gaining public attention. Companies need to ensure ongoing compliance in many business areas.

Compliance with laws and regulations is generally the responsibility of business management. Business management should lead the identification and implementation of good internal controls. Traditionally, internal audit organizations, IT compliance functions and public accountants have performed audits and reviews to measure compliance with company internal control processes, laws and standards.

However, audits and separate reviews determine internal control effectiveness only at a single point in time. Controls tend to degrade over time and between audits. With the current growing focus on internal controls, it is no wonder that both senior IT and finance management are now more interested in control monitoring.

WHERE TO START? MONITORING PROGRAM SPONSORSHIP

Strong sponsorship and tone at the top are required for an effective monitoring program. Unlike audits and separate compliance reviews, monitoring requires ongoing testing and evaluation. Detailed sampling and testing for a monitoring program may need to be performed by IT staff or those in business operations, rather than by corporate audit and compliance organizations. Management of the areas in the scope of monitoring programs needs to understand the benefits of the monitoring program. Having the support of senior management will help facilitate cooperation of staff members who will need to perform the monitoring process.

An easy-to-understand project plan or project charter will facilitate communication with senior management and the business operations areas under consideration for monitoring and include the following steps.

Step 1—Prioritize Risks

One of the challenges IT professionals may face when being involved in a monitoring project is linking IT risks to business risk. This requires focusing on IT processes to determine how the business may be affected by internal and external IT risk factors.

This involves understanding:

• Each business process and the role IT plays in that process
• The business objectives, related risks and key controls associated with the business process

Asking and answering questions such as the following can facilitate the IT professional’s understanding of the business process and the internal control environment:

• What is the objective of the business process?
• When and how does the process start? What are the triggers? Is there only one trigger or are there many? Have they all been identified?
• When and how does the process end?
• Which process steps or control activities are automated? Which are performed manually?
• Who performs the manual control activities?
• How is success (achievement of the predicted outcome) measured? Do the metrics cover the essential parameters to determine whether the objective is being met? These parameters include:
  • Effectiveness—Does it meet the output criteria (i.e., deliver what was ordered) with the promised quality and timeliness?
  • Efficiency—Are resources managed well?
  • Reliability—Does it meet specifications?
  • Other key factors—Are security, timeliness, confidentiality, integrity, availability and compliance addressed?
  • Who is accountable for the overall process performance?
  • Can process participants and their related roles and responsibilities in the process be identified?
  • What other information is utilized in the process?
  • Are significant risks related to the business process identified and prioritized?
  • Are control activities defined to address higher-priority risks?

Risks should be considered in the context of organizational/business objectives so they can be prioritized and appropriate resources can be allocated to manage them. A formal risk assessment can identify and evaluate the full range of risks against the stated business objectives and the enterprise’s unique business environment. It also can highlight functional areas that are most likely to impact enterprise objectives so that management can make informed choices about where to focus their monitoring efforts. No enterprise has unlimited resources. Information, people, applications and infrastructure allocated to reduce risk in one area inherently deplete resources that could be employed in other, potentially higher-risk areas.

**Step 2—Identify Key Controls and Information**

Start by identifying key controls in the process area under consideration for monitoring. In many organizations, processes have already been documented through past audits or compliance reviews. Using existing available documentation will help maintain focus on key controls—monitoring should focus only on key controls. Key controls are those that, if they fail, could materially affect the business objectives of the process or the organization. Past audits or reviews may help to identify controls that frequently fail or are more susceptible to business changes.

It is also important that the baseline of effective internal controls be identified and defined. The characteristics of the effective operation of the key controls identified need to be known to understand under what circumstances variation to the baseline would result in control failures. Past audit or review work can help to provide necessary information. By selecting key controls that address risks, management can efficiently focus its limited resources on high-value control activities.

**Figure 1** describes considerations relating to the complexity and maturity of business and IT process control types.

<table>
<thead>
<tr>
<th>Process Criteria</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>More complex</td>
<td>Use existing process documentation methodologies, such as Six Sigma’s Suppliers, Inputs, Process, Outputs, Customers (SIPOC), to identify controls that may benefit from monitoring.</td>
</tr>
<tr>
<td>Less complex (mature, routine or not complex)</td>
<td>Select monitoring activities that can be leveraged across multiple controls. Use existing technology or off-the-shelf tools for monitoring controls with minimal investment.</td>
</tr>
<tr>
<td>More mature (well defined and managed)</td>
<td>Integrate control monitoring into the daily business process operations (and the business process documentation) to add value.</td>
</tr>
<tr>
<td>Less mature</td>
<td>Once a control baseline is established, implement more frequent and stringent monitoring of the control until a control baseline is established.</td>
</tr>
</tbody>
</table>

Broad monitoring coverage for all key controls can be achieved by using a combination of direct and indirect information sources. Monitoring depth and frequency of specific key controls can be further determined by considering the following:

• How directly does the control support the relevant business objectives?
• What risks does the control address, and how important are they?
• Is the control considered a key control?
• What are the feasibility and costs of monitoring the control (using either direct or indirect information)?
• What is the nature of the control? Is it manual or automated, detective or preventive, etc.? If manual, is it dependent on IT information or an IT process for its effectiveness?
• If historical data are available, what is known about the maturity and past operating effectiveness of the control?

Once these factors are considered, the process of identifying the controls to be monitored and the information source for monitoring (direct or indirect) can begin. The following actions should be taken:

- **Identify controls that are in scope for monitoring**—Although key controls should be monitored, the degree of...
monitoring may vary based on the relative risk and value of each control. For example, those controls that address risks related to the most important business objectives and those that support multiple objectives may be monitored more extensively.

- **Determine the information sources available for monitoring**—Direct information is more effective than indirect information in ongoing monitoring and it usually allows for fewer separate evaluations. Information that comes directly from the control process is preferable to indirect information. Direct information is generally highly persuasive because it provides an unobstructed view of control operation; direct information comes directly from the execution of the control. In addition to direct information, however, indirect information such as key performance indicators (KPIs) may be useful. KPIs, as found in ISACA’s COBIT framework, can provide an excellent source for determining potential indirect monitoring measures.

In short, the management team expects that its most important processes will be both well defined and tightly controlled. The rigor of managing and measuring a process can vary, however, and depends greatly on how the enterprise interprets the relative importance of one process in comparison to others.

**Step 3—Implement Monitoring**

Implementing a monitoring program begins with the development of a project plan. Six Sigma and other project management methodologies provide excellent templates for planning and communication. Figure 2 provides an example of a practical project charter template.

Once the project plan has been developed, the process of determining the frequency for monitoring, developing the monitoring procedures and setting thresholds for monitoring that utilize indirect information can begin. The following actions should be taken:

- **Determine monitoring frequency**—A determination must be made regarding the use of ongoing monitoring, separate evaluations or a combination of both techniques. When ongoing techniques utilize highly persuasive information (i.e., direct information), they can routinely provide evidence that a control is operating as intended. If they use less persuasive information (i.e., indirect information),

![Figure 2—Attributes of a Monitoring Project Plan](image)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business case</td>
<td>Describes the benefits for undertaking a monitoring project. Why is this monitoring project important to the enterprise? What are the risk implications of the failure of key control(s) selected for monitoring? Why is it important to do it now? How does the monitoring project align with enterprise goals? What are the consequences of not doing this monitoring for the enterprise?</td>
</tr>
<tr>
<td>Problem/opportunity</td>
<td>States what problems or needs the initiative will solve and clarifies the “why” of undertaking the project. For example, control failures within the software change management process can result in processing errors and other control failures affecting enterprise operations and can make excessive programming rework necessary within the IT department.</td>
</tr>
<tr>
<td>opportunity statement</td>
<td></td>
</tr>
<tr>
<td>Goal statement</td>
<td>Defines the objective of the project in measurable terms. The goal statement should solve the potential problems identified in the problem/opportunity statement. The goal statement provides direction for detecting control failures, leading toward solutions. For example, monitoring of key controls within the change management process—specifically, the use of formal change request forms, approval of change requests by authorized personnel and testing of all changes in compliance with enterprise policy—will increase system reliability, help availability, decrease rework and help contain cost.</td>
</tr>
<tr>
<td>Scope</td>
<td>Defines the boundaries of the project and should answer the following questions: • What parts of the enterprise or business processes are included in the scope? • Where will the work be performed? • What parts of the enterprise or business processes are not included in the scope? • What is the role of IT and users in this project? • Can the project be subdivided so that a pilot area can be reviewed first to test the assumptions, data collection and testing processes?</td>
</tr>
<tr>
<td>Approach</td>
<td>Defines the information, methods and tools selected for monitoring projects. The type of sampling may also be documented.</td>
</tr>
<tr>
<td>Timeline and budget</td>
<td>Documents the major milestones, timing and estimated costs for the project. At a minimum, the plan should consider the time for the design, implementation, testing and periodic follow up on results. It should also identify any out-of-pocket costs that may be incurred, including any ongoing maintenance costs and, if appropriate, internal personnel costs.</td>
</tr>
<tr>
<td>Project team</td>
<td>Identifies the monitoring team. The team members should include people with a good knowledge of the business process. They should have IT skills that enable them to understand the IT processes and controls. If specialized IT automated audit tools are required to obtain sample transactions for review, someone on the team needs to have the skills and experience to develop the automated testing process.</td>
</tr>
<tr>
<td>People accountable and</td>
<td>Identifies the senior management personnel who are accountable for the monitoring project, and identifies the leaders of the monitoring project and key members of the business process teams involved in the monitoring</td>
</tr>
<tr>
<td>responsible</td>
<td></td>
</tr>
<tr>
<td>Evaluation and feedback</td>
<td>Identifies how project success is going to be measured. It may consist of nothing more than reviewing the results of the monitoring activity and determining whether the goals of the project were realized. For example, using the goal statement example, evaluation may consist of review, on a periodic basis, for positive changes to the metrics around system reliability, help availability, rework and cost containment.</td>
</tr>
</tbody>
</table>
additional separate evaluations may be required more frequently. In both cases, separate evaluations may be required periodically.

Automation is another consideration in determining the frequency of monitoring. In general, based on the assessed level of risk (key control or not), automated controls require less frequent monitoring of their automated aspects because once the control is verified to be working properly, automated aspects are unlikely to change unless change management controls cannot be relied upon. Nonautomated aspects, such as follow-up on reported exceptions, may require more frequent monitoring, depending on the risks. An automated control may allow for even greater usage of indirect information, once the initial baseline for using direct information has been established, as system controls are less likely to degenerate than manual controls if—and only if—the underlying IT general controls are effective.

- **Develop monitoring procedures**—A monitoring procedure needs to be developed for both ongoing and separate evaluations. The project plan should specify the information source to be utilized for each approach. Enterprises using indirect information as a source for ongoing monitoring will still find it necessary to perform a separate evaluation using more persuasive or direct information. In addition, monitoring procedures that provide comfort over more than one control may be given preference over more targeted procedures (e.g., the review of a change control ticket may provide evidence of business sign-off, testing results and the existence of a back-out plan).

- **Determine thresholds for monitoring when utilizing indirect information**—Indirect information cannot provide positive assurance that a control is operating effectively; however, indirect information can be a good indicator of the effectiveness with which the process meets its overall performance objectives. If such indirect information suggests that the performance objectives are not being met, this may indicate that the related key controls are not functioning effectively. A tolerance window for the deterioration of a key metric or indirect monitoring should be established to trigger the need for direct monitoring or other follow-up action.

To be successful, accountable process owners need to be able to rely on the monitoring process itself for reliable results. Consequently, their involvement is essential during the development process and once the monitoring process is operational.

To ensure correct results and conclusions, the monitoring process must be repeatable and it must minimize the variations in how monitoring is performed. In cases in which a monitoring process is critical to an enterprise, it may be necessary to implement controls over the monitoring process itself to detect and manage variability in how the data are extracted, validated, analyzed and reported.3

Wherever possible, monitoring programs should leverage automation. Automation of testing can reduce the effort needed to perform internal control monitoring and reduce resistance to implementation of a monitoring program. Automated monitoring is less likely than manual monitoring to produce variations in the monitoring processes. As stated previously, effective IT general controls must be in place for development and subsequent operation of automated monitoring solutions. These include controls over software development, software maintenance, and system and user testing. Such controls are covered in detail in various ISACA publications, such as COBIT® 4.1, Enterprise Value: Governance of IT Investments, The Val IT™ Framework 2.0 and the IT Assurance Guide: Using COBIT®.

After monitoring program design and implementation are complete and the system is operational, processes need to be in place to monitor and assess the results. Although testing would have been performed to validate functionality during development, ongoing activities that need to be considered include:

- Reviewing the monitoring results to minimize false positives or negatives and to ensure valid, current and timely results.
- Control failures may be reported when, in fact, they are not failures because the business itself has changed. This would be more likely to be true with continuous controls monitoring solutions vs. manual monitoring processes.
- Determining the reason for the control failure
- Reporting results back to the project sponsors, along with any recommendations, so they can implement corrective actions.

Once the monitoring process flags a potential control failure, identifying the root cause will aid in defining appropriate corrective actions. The goals of root-cause analysis are to identify and correct the primary reason for the failure of the controls. More information may need to be gathered, such as when, where and how the failure occurred. Did it occur because of a recurring condition that could be resolved by process improvements, or was it due to a less common or special circumstance that would have been difficult to predict or anticipate? Further testing or sampling may be required to determine whether the failure is repeated.
It is important to identify the appropriate levels of enterprise management that must be informed about the condition or event, the type of corrective action that is or will be taken, and the expected time frame for mitigation (assuming it is not postrecovery). Management should receive information that is clear and concise (preferably stated in nontechnical business terms) to enable efficient and effective understanding of the impact to the enterprise and clients.

As a minimum for reporting, the results of monitoring should include the items listed in figure 3.

<table>
<thead>
<tr>
<th>Item</th>
<th>Related Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem statement</td>
<td>Identify the problem, e.g., control failure.</td>
</tr>
<tr>
<td>Cause identification</td>
<td>Describe the root cause of the control failure.</td>
</tr>
<tr>
<td>Perspective on risk</td>
<td>Describe the risk to the business process created by the control failure. For example, the risk may be lack of compliance with a particular standard or regulatory requirement. Also, describe any adverse consequences that might have occurred.</td>
</tr>
<tr>
<td>Recommendations</td>
<td>Identify the corrective action, including what is to be done, by whom and by when (estimated completion date). Any follow-up actions should also be discussed.</td>
</tr>
</tbody>
</table>

Any warranted and cost-justifiable changes should be noted, and any changes resulting from corrective actions taken should be mapped back to any processes affected. Documentation should be updated and appropriate personnel notified. Also, the monitoring process should be regularly reviewed to help ensure that the monitoring process and the controls it monitors continue to operate effectively.

**CONCLUSION**

Senior management is interested in saving time, money and other resources in business processes. Finance and IT management want to know that internal controls under their responsibility are operating effectively at all times. Internal audit and IT governance personnel can meet the needs of their management through the development of efficient and cost-effective internal controls monitoring programs.

To develop a good internal controls monitoring program, the following are needed:

- Management sponsorship and tone at the top
- An understanding of business processes, objectives and organizational structure
- An established baseline of effective internal controls from the past or from a current review
- Identification of key controls and prioritization of risks
- Identification of information for monitoring controls (direct information is best)
- A good project plan and implementation of monitoring
- A report on the findings of the monitoring processes
- A follow-up process for corrective actions

**EDITOR’S NOTE**

The new ISACA publication *Monitoring Internal Control Systems and IT* is available in the ISACA Bookstore and posted for complimentary download on the ISACA web site, www.isaca.org.

**ENDNOTES**

1 *CFO Magazine*, 10 December 2009
2 *CFO Magazine*, 12 January 2010
3 An analytically based process is available to help ensure the accuracy of monitoring. Measurement Systems Analysis (MSA) is a Six Sigma-based process for analyzing the monitoring processes for potential variation and defects. For further information on how to create and use an MSA process, refer to a Six Sigma Black Belt resource or to web sites such as iSixSigma.com.