A LOOK INTO THE FUTURE: THE NEXT EVOLUTION OF INTERNAL AUDIT
CONTINUOUS RISK AND CONTROL ASSURANCE
About the Author

Before joining the governance, risk, and compliance (GRC) solutions team at SAP, Norman Marks was the leader of internal audit functions at major U.S. and global corporations for more than 15 years, also serving at times as chief ethics and compliance officer and chief risk officer. He is a recognized international leader in the theory and practice of internal auditing and was profiled by the magazines of the American Institute of Certified Public Accountants and the Institute of Internal Auditors (IIA) for his innovative practices. He is the author of some of the IIA’s most downloaded publications, including Sarbanes-Oxley §404: A Guide for Management by Internal Controls Practitioners.
The not-too-distant future for internal auditing includes a technology-driven revolution that will enable a dramatic and necessary change in the way internal auditors operate. The internal auditing function will be able to provide almost continuous assurance that risks of significance are effectively managed and that related controls are performing as desired across the organization.

Traditional assurance projects will largely be replaced by a combination of continuous auditing and monitoring and rapid-response audits of risk hot spots. Resources will be freed up for process improvement and other consulting opportunities. Many of the seeds of that change have already borne fruit that is ready to be reaped today.

Our vision is illustrated through the telling of a story, set a few years from now, by the fictional Charles Andrew Edgar, senior vice president of internal audit for Tap Toes Inc., a global shoe-manufacturing company based in San Francisco.
"This morning my quiet breakfast was interrupted by a loud chirp from my smart phone. I answered immediately, as it was the special tone I had set for alerts from our continuous risk and control assurance system.

"The alert told me that one of our continuous audit and monitoring routines had detected an unusually large physical-inventory variance in our Blackpool, England, location. Clearly, my normal morning routine was going to change.

"The message included a detailed description of the alert, but even with today’s technology, the screen on the smart phone was too small for me to read comfortably. I took a cup of coffee into my home office and, after going through the normal security protocols, opened the alert on my laptop.

"Apparent ly, a routine monthly physical-inventory check in the Blackpool location had identified a large discrepancy in the finished goods inventory of ballroom dancing shoes. The Blackpool finance director had posted a journal entry writing off the shoes, which our monitoring had detected. The shoes are expensive, so the write-off was above the thresholds (dollar and percentage) we had set our software to monitor.

"I used a hyperlink in the message to enter the corporate risk and control system (CRCS), which drives our continuous assurance program. CRCS monitors the health of the more significant risks (in this case, those related to the safeguarding and accurate reporting of inventory) and related controls.

"First, I checked out the general level of risk at the Blackpool location, as that would give me an idea whether there was any indication of employee dissatisfaction or other situation that could lead to theft. I found that:

- General risk levels related to the Blackpool location were recently raised due to UK press reports that the Blackpool plant might be closed. (We have standard feeds from commercial news agencies and supplement them with our own search engine. The data is both structured, such as government employment reports, and unstructured, such as articles in the local press. The results are collected and analyzed in the corporate data warehouse and links added to the risk management system.)
- The latest human resources department employee surveys did not identify any elevated employee concerns. In general, it appeared employee morale was good, in line with the rest of the organization.
- There had not been any significant change in personnel turnover, including in management.
- The most recent external audit had not identified any issues. In addition, there were no open remediation items – from external audit, internal audit, or other assurance functions.

(By the way, all our assurance functions – such as the corporate compliance and corporate quality teams, as well as internal auditing – use CRCS and its multicompliance framework for risk identification and assessment, audit planning, tracking of audit results, and the monitoring of remediation items.)

- The internal audit team had been to Blackpool 18 months ago. As with most of our on-site audits, the latest was an operational audit. This particular audit was of the lean finance operation (several of the internal audit team are Lean Six Sigma Black Belts) and the resulting assessment was positive. There were no deficiencies of significance.

"I moved from the top-level Blackpool risks to a view that focused on inventory risks. I first checked out the risk of inventory theft. Our continuous assurance program is driven by a top-down, risk-based process for identifying the key controls relied upon to achieve the company’s strategic objectives. For each of the objectives, we worked collaboratively with management and the risk officer to identify the risks to achieving the objectives. Then we determined the strategy or response to be followed to manage each risk (transfer or share, avoid, reduce or mitigate, or accept) and the controls required to ensure that the strategy is effective. Finally, we implemented continuous testing for each of the controls."
"The dashboard for the controls showed green lights across the board. Notably:
- There were no other unusual inventory transactions such as physical-inventory variances in prior months, write-offs for quality, transfers between locations, inventory reclassifications, or transactions posted directly by IT.
- The individuals accessing the inventory records did not have incompatible functions. (Ours is a real-time test, rather than the after-the-fact analysis and reporting that was popular five years ago.)
- All new access rights granted to the inventory records were approved by appropriate senior management, and no new inventory access rights had been granted in the last quarter.
- Prior monthly physical inventories had been performed as scheduled without significant variances, and the results were approved by appropriate senior management.
- Related application controls were reliable. These included, for example, controls to ensure that inventory records agree with the general ledger, opening inventory plus purchases less sales and adjustments equals closing inventory, shipments cannot be made in excess of sales orders, and so forth. This was based on continuous testing of IT general controls, such as approval for configuration or code changes, and reperformance of selected key application controls.
- Access to the physical inventory was limited to employees with appropriate business needs. This was achieved through an automated test. We extracted from the security system, on a weekly basis, a list of employees who had access to the inventory and verified their business need (based on a lookup of HR system records).
- The risk management system had more details on assessments by the other assurance providers, including a copy of the last quarterly inspection by corporate security.\(^2\) The corporate security team had assessed the risk from inventory theft to be low. All the cameras were in place and working properly, management and employees demonstrated the appropriate level of attention to security, and the inventory was properly secured. The Blackpool security team was at full strength, and only current employees had access to the finished goods inventory.
- To add perspective, I reviewed the latest financial performance results:
  - The Blackpool location has been consistently profitable, although the results in the last quarter were 5% below forecast.\(^3\)
  - The inventory write-off was substantial but less than 5% of total inventory, causing the plant to have a small loss for the quarter.\(^4\)
  - Sales were quite seasonal, with the highest volumes in the fall. Inventory balances were consistent, with sales at their highest just before the sales peak and at their lowest in the following quarter.
- The auditor assigned to monitor Blackpool operations and risks was Fred Eagle. (Each member of our team is assigned to work with the management of selected locations or functions
to understand the business and its more significant risks. In the old days, we updated the risk-based audit plan formally once a year and informally every quarter. Now, I expect it to be updated weekly in CRCS by the audit team.) Fred had confirmed the internal audit risk assessment as low just last week.

“I called Fred and we talked about what to do. We agreed the first step was to check that the other Blackpool inventory risks were all green lights and that the updates were current. We were interrupted by a call from the logistics manager. I put him on hold while I asked Fred to check out the other controls and call the Blackpool controller to get a status report. In particular, Fred was to confirm that the physical inventory count had followed the correct procedures.

“The logistics manager told me that he had also received an alert. He was concerned that we did not have sufficient inventory on hand in Blackpool to fill a large order from an important customer. He was glad to know that we were already looking into the situation and asked that we let him know as soon as possible what the resolution was, so he could work something out with the customer.

“About an hour later, Fred called back. He said that automated continuous assurance only goes so far. It’s like having a patient in the intensive care unit of the hospital: the patient’s vital signs might be electronically monitored, but every so often a nurse needs to check in to make a physical observation. The situation in Blackpool was the same: all the monitors indicated that the controls were working fine, but sometimes you need that in-person contact.

“In this case, Fred and the local controller convened a meeting with the inventory, operations, and finance staff. Fred walked them through the processes they had followed to perform the inventory and found a problem with their cutoff procedures. They had not checked to ensure that all the inventory movements were in the system. In response to Fred’s questions, they realized that one of the shipping clerks had taken ill the day before the inventory count. The controller made a call and confirmed that a couple of pickups by the carrier had not been processed. The amounts involved were almost exactly the inventory shortage.

“The problem was solved, and Blackpool management agreed to improve processes for future inventory counts. In the meantime, Fred and I talked about whether we should add automated risk-monitoring procedures for inventory counts and then start continuous auditing for related controls. We decided that the current inventory risk monitors were sufficient. That is consistent with our whole approach to continuous assurance: focus on the more significant risks and improve the program over time as we learn from experience.”

The Journey from Traditional Auditing

Edgar describes how his company developed the continuous risk and control assurance program.

“For years before we started our program, the internal audit community had been very interested in continuous auditing and monitoring. (There is no fundamental difference between the two. The distinction lies not in the work being performed but in who is performing it: ‘auditing’ by internal audit and ‘monitoring’ by management.) The value was seen in:

• Automating certain control tests where there was a need to test every year – for the annual Sarbanes-Oxley assessment of internal control over financial reporting, for instance
• Testing data and gaining insight into related controls in more sensitive business processes such as accounts payable and payroll, particularly where there was a risk of fraud.

“The focus was on using automation to test controls and examine data, but there was no linkage to or focus on risk. In addition, a number of internal audit leaders had been talking for a long time about the fact that our role in internal audit is not to perform audits. In fact, our role is to provide the board and executive management with assurance that the organization’s risks are understood and managed within board-established risk tolerances, and that the system of internal control is operating as intended.
The Institute of Internal Auditors’ Standards defines internal auditing as an activity that ‘provides independent, objective assurance and consulting services.’ Emphasis is added.) We recognized that providing this peace of mind – the ability to ‘sleep during the storm’ – could best be done through continuous risk and control assurance. We define this activity as follows:

The ability to provide stakeholders with assurance on a continuing basis that the more significant risks are managed and related controls are operating effectively.’

“We worked with management, especially the risk management team, to identify the areas of greatest risk to the company’s objectives. The risk management team agreed to implement a continuous risk-monitoring program to measure and report the status of those risks. Next, we identified the key controls required to manage those risks. For each, a strategy was developed: how would we monitor the performance of the controls? Where possible, we automated the testing of the controls (which often included auditing of related transactions or activities). The results of the monitoring activities were used to maintain, in part, the risk status.

“The continuous risk and control assurance program provides management in all areas with reports and dashboards showing the status of all the key risks. Where there are adverse incidents, potential control breakdowns or frauds, or risks appearing to spike upward, internal audit and responsible management receive immediate alerts, such as the one I received during breakfast.

“Our program enables us to give management and the board the continuous assurance they value so highly. It also enables us to move to more of a ‘monitor and respond’ approach in the assurance area and focus our project time on issues and opportunities to drive process efficiencies and other improvements in the operation of the company.

“The success of our continuous assurance program has been significantly enhanced by the GRC convergence program we conducted at about the same time. All the functions involved in GRC work together to avoid duplication of effort, rely on each others’ work, and use the same systems and processes where possible. In our case, that involves internal audit, risk management, supply and logistics, physical security, IT governance, legal compliance, and financial compliance (Sarbanes-Oxley, tax and statutory reporting, and so on).

“As internal auditors, we are obliged to provide independent and objective assurance to our stakeholders. Where we have decided to rely on other assurance providers’ work, we make sure we have performed procedures ourselves to give us reasonable assurance of the quality and consistency of that work. So we perform periodic audits of the risk management office, corporate security, IT security, and the like.

“Convergence involved process and tools. While we considered integrating some of the GRC functions, in the end we decided to keep them independent but cooperating. From a process point of view, we all decided to take a risk-based approach, especially around compliance topics. Legal compliance might identify a high-level risk related to compliance with U.S. technology export laws, for example. That would be identified as a risk in our risk management system, where we would also identify the controls in place to manage the risks. The level of risk, the number and severity of any adverse incidents, the controls in place to manage the risks, and corrective actions (where issues are identified) are all monitored and tracked in the same system. This approach provides the legal compliance and risk management leaders with a single source of truth about the risk level and how well it is managed. It also enables all the operational managers responsible for any of the processes involved, such as supply and logistics, to include monitoring of this risk in their daily, weekly, and monthly dashboards.

“The tools are also shared: we use a number of products from SAP, including SAP® BusinessObjects™ GRC solutions for risk management, access control, process control, and global trade services. We also use SAP BusinessObjects business intelligence solutions to drive our corporate and internal audit data warehouses, and SAP BusinessObjects Text Analysis software for Web-based searches of unstructured data.
“The internal audit department had received overtures from a number of vendors offering excellent point solutions designed for internal audit functions or specifically for internal control or data auditing. However, we placed a high value on avoiding software proliferation in favor of using common enterprise applications.

“We perform a large number of audit projects that focus on operational effectiveness and efficiency. We can do this because the continuous assurance program is highly effective. A comparatively small portion of our time is spent on assurance, freeing up the audit staff for value-added consulting projects. The audit committee and executive management have confidence in our risk management and internal control processes and have made it a priority for internal audit to perform these projects.

“The results of our consulting projects sometimes indicate an opportunity to improve business processes or operations, which we capture in our risk management system. After all, efficiency is a corporate objective, and we can identify and monitor related risks.

“In the old days, when we performed traditional assurance projects, we had an audit management system. It was a software product where we maintained our work papers, tracked the history of our audits, followed up on audit findings and management actions, and generally managed the audit team – project planning, skills inventory, and the like. The continuous assurance program has eliminated most of that, as follows:

- The results of any audit work, including risk and control assessments, are captured in the risk management system. The history is automatically captured.
- We also track corrective actions in the risk management system.
- Project planning, where needed, is done using specialized project management software.
- The skills inventory, which is very important to our ability to staff projects like lean finance or inventory management, is maintained in our SAP ERP Human Capital Management solution.”
Edgar’s story is typical of the internal audit executive of the future. In its breakthrough paper, *Internal Audit 2012,* PricewaterhouseCoopers discussed a “consensus projection of the trends likely to shape the world of internal audit by the year 2012.” Of particular note are the following observations (emphasis added):

“Throughout the next five years, the value of the controls-focused approach that has dominated internal audit is expected to diminish. As this occurs, internal audit leaders must adopt risk-centric mind-sets if they want to remain key players in assurance and risk management.”

“Some internal audit functions have begun to rethink their fundamental value propositions by shifting from an internal audit model focused on controls assurance to a risk-centric model where risk and control assurance are based on the effectiveness of risk management processes developed by management.”

“One of the five key trends that will drive this reshaping of internal audit by 2012 is technological advancement.”

Deloitte & Touche has a similar perspective, according to Patty Miller (a partner and chairman of the Institute of Internal Auditors for 2008–2009). She uses the following table to illustrate the major changes happening in internal auditing.

There are multiple points of interest in the Deloitte vision:
- The focus is on risk, with a forward-looking and proactive style and dynamic reporting.
- The mandate is business assurance, similar to risk and control assurance.
- The technology application of greatest importance will be automated testing and continuous monitoring.

While there is a need for risk and control assurance, we believe that the optimal model for the future is one of continuous assurance of risk and control. This is consistent with guidance from the Institute of Internal Auditors, which focuses on the provision of assurance rather than the performance of audits.

Internal audit will provide its customers, the board of directors, and executive management with assurance that the organization’s risks are subject to appropriate and effective processes, including related systems of internal control. The assurance will be enabled primarily through continuous risk and control monitoring and auditing, with a much reduced set of traditional audit projects.

<table>
<thead>
<tr>
<th>Table 1: Changes Taking Place in Internal Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus</td>
</tr>
<tr>
<td>Focus</td>
</tr>
<tr>
<td>Perspective</td>
</tr>
<tr>
<td>Style</td>
</tr>
<tr>
<td>Mandate</td>
</tr>
<tr>
<td>Risk Focus</td>
</tr>
<tr>
<td>Tool Kit</td>
</tr>
<tr>
<td>Technology</td>
</tr>
</tbody>
</table>
Model Overview

Figure 1 illustrates the continuous risk and control assurance model. It is far more than an application of continuous auditing or monitoring. Rather, it is a top-down model that starts with understanding enterprise goals and objectives, moves on to determine the potential risks to those objectives, and then moves to the assessment and testing of the controls required to manage the risks. The overall effort usually encompasses the mining of data that can provide indicators of the health of risk management and related controls.

The model’s foundation is built upon the more significant strategic and operational goals of the enterprise. Achievement of the goals and objectives is measured through key performance indicators (KPIs). The model includes the monitoring of KPIs, as the failure to achieve organizational objectives is often the result of poor risk management or control performance.

Risks to the achievement of those goals and objectives are then identified. Continuous risk monitoring, generally by a risk management function and not by internal audit, ensures that the program is focused on the more significant risks to the enterprise, which may change rapidly. Internal audit is a consumer of the monitoring but not responsible for its performance.

Management of those risks – risk responses – is enabled by controls. The model includes the continuous auditing of the key controls required to manage risks within organizational tolerances, usually performed by internal audit and other assurance providers, sometimes by operating management.

Some controls are difficult to test directly through automated routines, and the continuous examination or testing of data may provide a reasonable level of assurance. The data mining may be directly against information within the organization’s applications or indirectly after extraction to a data warehouse (either an existing corporate data warehouse or one developed specifically for this purpose).

Fraud management is built into the program:

- Fraud risks are identified together with other enterprise risks.
- The controls over fraud risks are assessed and tested together with other key controls.
- Data mining techniques can be used to test data and identify potential fraud situations.

![Figure 1: The Continuous Risk and Control Assurance Model](image-url)
When assurance is continuous, information on the health of risk management and related key controls needs to be continuously available to stakeholders. The model encompasses continuous reporting through dashboards or similar tools. It also includes more immediate alerts signaling the need for a response to a spike in risk levels, an adverse incident, a potential controls failure, or a data anomaly.

On-demand data mining enables an intelligent response and investigation of data anomalies, control failures, and so on. The same tools that provide continuous control and data auditing will generally also support additional data analytics that provide further insight into the problem.

Each of the major elements of the model is discussed in more detail below.

Continuous Risk Monitoring

The continuous risk and control assurance program relies on the quality of the enterprise risk management process established by company management. This process identifies and assesses the risks to enterprise objectives to be covered by the assurance program. Although internal auditors may have an independent assessment of risks (based on their experience, for example), the auditors’ rating should be integrated with, or at least be a revision to, the assessment of the management team, rather than the result of a separate and potentially redundant risk assessment process. Internal auditors can (and should, according to IIA standards) gain comfort in the risk management process through periodic audits. These audits should address the adequacy of the process established by management to identify and assess risks to achieving organizational objectives. Importantly, the audits should evaluate whether the risk assessment considers all factors that internal auditors believe relevant to the risk assessment, such as the results of prior internal audits and the status of open action items.

Most organizational objectives remain relatively constant; typically, organizations only review them annually unless there are major changes in business conditions. But risks to the organization change constantly. New risks emerge while old ones fade in importance, and existing risks rise and fall as business conditions change. Continuous risk monitoring is required to:

- Ensure that assurance is provided on today’s more significant risks
- Identify new or growing risks that require additional risk and control monitoring
- Identify sudden rises in risk levels that may merit immediate attention by management or internal auditors. The large inventory write-off described earlier led to an increase in inventory-related risk levels. The internal audit team responded because this might signal a breakdown in related controls and the potential for additional inventory losses.

Management is typically responsible for monitoring risks, while the internal audit department is a consumer of risk information. The ability to monitor risks will become more effective when technology is used to:

- Link enterprise information (such as financial results, account balances, and health and safety information) with the risk management process. For example, if Tap Toes Inc. substantially increases sales to China, that should result in an increase in related accounts receivable risks.
- Link external information to risk assessment processes. Many enterprise risks relate to external events, and geopolitical or economic changes may indicate a need to change risk levels. For example, civil unrest in an emerging nation may indicate the need for Tap Toes to change risk levels if the company relies on manufacturing operations in the area.

These technologies are available today, and their ease of use and integration into solutions should improve over the next few years. The results of risk monitoring (including key risk indicators) would typically be shown in dashboards and other reports to the board and to executive and operating management.
Those dashboards enable the monitoring of risk levels and taking of action where needed.

In addition, alerts should be provided to appropriate management and internal audit teams when there are sudden changes in risk levels warranting more immediate action. Typically, the internal audit team will review the alert to determine whether there has been a breakdown in either risk management or the related internal controls. In some cases, audit projects and even investigations may be required to assess the situation and identify remedial actions.

Continuous Controls and Data Auditing

The continuous assurance program should focus only on the more significant risks and related controls. Once the risks to be included in the program have been identified, the controls and data to be tested can be defined. The selection process for risks to be included should consider:

- The highest-rated risks
- Risks that may not be likely but where an adverse incident could be a threat to the entire enterprise
- Areas where key stakeholders (such as the board or executive management) place a high value on assurance

Once the business risks are determined, the next step is to identify the key controls required to manage those risks within organizational tolerances. In almost all cases, organizations rely on a combination of controls to manage a business risk. Most risks will depend on controls at the entity level (a code of conduct, a corporate policy, and so on), in business processes (accounts payable, for example), and within IT processes (such as application change control or security).

It is critical to understand all the key controls, since an assurance strategy has to include measures to obtain assurance for them all. Table 2 lists some of the key controls to manage the risk of theft of finished goods inventory at a hypothetical company.

### Table 2: Example of a Combination of Key Controls

<table>
<thead>
<tr>
<th>Controls</th>
<th>Type of Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>The organization has a code of business conduct.</td>
<td>Entity-level</td>
</tr>
<tr>
<td>New employees are required to confirm their understanding of the code of conduct. Records are maintained in the HR system.</td>
<td>Entity-level</td>
</tr>
<tr>
<td>All employees sign a code of conduct certification annually and records are maintained in the HR system.</td>
<td>Entity-level</td>
</tr>
<tr>
<td>Hiring procedures include background checks, with records maintained in the HR system.</td>
<td>Entity-level</td>
</tr>
<tr>
<td>Physical access to finished goods inventories is restricted based on business need.</td>
<td>Business process</td>
</tr>
<tr>
<td>Finished goods inventories are physically secured by doors and monitored by guards; cameras are in place.</td>
<td>Business process</td>
</tr>
<tr>
<td>After inventory counts are entered, the inventory module provides reports showing inventory variances. Each report shows the inventory per the system, the inventory counted, and the calculated variances.</td>
<td>Business process</td>
</tr>
<tr>
<td>Only the inventory manager can approve the posting of inventory adjustments (for example, write-offs following the inventory count).</td>
<td>Business process</td>
</tr>
<tr>
<td>All inventory program changes are approved by the inventory manager in the change control system.</td>
<td>IT general control</td>
</tr>
</tbody>
</table>
Some of these controls are difficult to test directly on a continuous basis, and it may be better to test the underlying data. For example, the second control above is “New employees are required to confirm their understanding of the code of conduct. Records are maintained in the HR system.” In a traditional assurance project, the auditor would review the employee records and confirm, through examination of a sample of documents, that the employee had signed to confirm understanding. In a continuous assurance program, examination of signatures is unlikely to be an option. Instead, the HR system records might be tested to identify new employees where there was no record of a confirmation (a data auditing or data mining technique). The level of assurance is not as strong as if the actual signatures were tested, but the auditor may decide that a reasonable level of assurance is obtained that can be upgraded by adding an annual examination of signatures (if the auditor determines the risk so merits).

The auditor may assess as low the risk of noncompliance with a control or the risk presented if the control was ineffective. In these cases, the auditor may decide that sufficient assurance is achieved by a less-frequent test strategy. An example would be the first control above: “The organization has a code of business conduct.” Because the second control is tested, there is a high degree of assurance that the code of business conduct exists and is available to employees. The auditor may decide not to test the control directly or to test it only annually.

It is generally best to test data as it is being processed by the application system; if there are questionable results, they can be investigated promptly and adverse consequences can be prevented or at least minimized. However, there are times when it may be better to use data that has been extracted to a data warehouse for testing. (This data may be in an existing data warehouse or in one developed for this particular purpose – perhaps owned by the internal audit department.) An example is where the auditor wants to test trends over a period of time. The use of a data warehouse may also be valuable when data is being compared to information in other systems. For example, access to an inventory warehouse should be limited to individuals with warehouse responsibilities, which can be identified through information in each person’s HR records.

The key is that the auditor will consider each of the key controls relied on for the risk to be addressed and determine the specific assurance strategy and the specific assurance technique. (For example, the strategy might be to test the control, test the data, or rely on the work of other assurance providers.) Table 3 takes each of the controls in Table 2 and assigns a strategy and continuous assurance technique.

Key points from the example include:
- Assurance is obtained using a combination of techniques, including automated and nonautomated testing (such as the annual review of the code of ethics), the testing of controls and data, and reliance on other assurance activities (such as SOX testing and corporate security audits).
- Not all the techniques are continuous in nature (for example, the periodic testing of HR record keeping).

This particular example brings out a limitation in most audits of internal control, whether using continuous assurance techniques or traditional auditing methods: the difficulty in auditing behavioral aspects of internal control. Do the people who have signed a certification of the code of conduct actually understand and intend to follow the code of conduct? The latter, which involves the integrity of individual employees, is hard if not impossible to test; instead, controls that provide reasonable assurance, such as background checks, are assessed. However, it is possible to test with reasonable effectiveness whether individuals understand the code of conduct: through interviews during traditional audits or through online testing. Employees might be asked to answer questions about the content or the location of the policy included in continuous audit assurance programs.
## Table 3: Example of Key Controls and Assurance Techniques

<table>
<thead>
<tr>
<th>Controls</th>
<th>Assurance Strategy</th>
<th>Assurance Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>The organization has a code of business conduct.</td>
<td>Annual test by examination</td>
<td>Review the code of conduct and ensure it is current</td>
</tr>
<tr>
<td>New employees are required to confirm their understanding of the code of conduct. Records are maintained in the HR system.</td>
<td>Continuous data auditing of HR records</td>
<td>Identify any employees who have not confirmed the code of conduct within 3 months of hire, according to HR records</td>
</tr>
<tr>
<td></td>
<td>Periodic auditing of HR system maintenance procedures</td>
<td>On a periodic basis, validate that HR records are updated accurately and on a timely basis</td>
</tr>
<tr>
<td>All employees sign a code of conduct certification annually and records are maintained in the HR system.</td>
<td>Continuous data auditing of HR records</td>
<td>Identify any employees who have not certified the code of conduct as required</td>
</tr>
<tr>
<td></td>
<td>Periodic auditing of HR system maintenance procedures</td>
<td>On a periodic basis, validate that HR records are updated accurately and on a timely basis</td>
</tr>
<tr>
<td>Hiring procedures include background checks, with records maintained in the HR system.</td>
<td>Continuous data auditing of HR records</td>
<td>Identify any employees where a clean background check is not recorded in the HR system</td>
</tr>
<tr>
<td></td>
<td>Periodic auditing of HR system maintenance procedures</td>
<td>On a periodic basis, validate that HR records are updated accurately and on a timely basis</td>
</tr>
<tr>
<td>Physical access to finished goods inventories is restricted based on business need.</td>
<td>Continuous data auditing</td>
<td>Identify any individual whose badge grants access to finished goods inventory but who does not have a business need based on job function (per HR system)</td>
</tr>
<tr>
<td>Finished goods inventories are physically secured by doors and monitored by guards; cameras are in place.</td>
<td>Reliance on physical security audits by corporate security, together with monitoring of security audits</td>
<td>Obtain an alert whenever a security audit report is filed by exceptions</td>
</tr>
<tr>
<td></td>
<td>Continuous data auditing</td>
<td>Identify any delays in filing the results of security audits (required at least quarterly)</td>
</tr>
<tr>
<td>After inventory counts are entered, the inventory module provides reports showing inventory variances. Each report shows the inventory per the system, the inventory counted, and the calculated variances.</td>
<td>Reliance on annual Sarbanes-Oxley (SOX) reperformance of application controls</td>
<td>Include reperformance of the inventory variance calculation in SOX testing</td>
</tr>
<tr>
<td>Only the inventory manager can approve the posting of inventory adjustments (for example, write-offs following the inventory count).</td>
<td>Continuous control and data auditing</td>
<td>Continuously test access control procedures, including that no changes are made to authority to approve inventory adjustments (an exception report is sent to IT security and internal audit if there are changes)</td>
</tr>
<tr>
<td>All inventory program changes are approved by the inventory manager in the change control system.</td>
<td>Reliance on annual SOX testing of IT general controls</td>
<td>Include continuous data testing in SOX testing: only the inventory manager approves program changes</td>
</tr>
</tbody>
</table>
Continuous Fraud Detection

Fraud is one risk that needs to be addressed by every organization. In general, the level of effort should be commensurate with the level of risk and the risk tolerance of the organization.

Fraud detection is one element of an effective fraud management program, and it is more efficient when integrated with the continuous risk and fraud assurance program. For example:

- Fraud risks are monitored with other organizational risks to ensure that fraud detection activities address current risks.
- Controls to prevent or detect fraud are assessed, as with controls related to other risks.
- Continuous fraud detection is primarily performed using the same continuous data mining and other testing techniques.

The level of frauds detected by the normal operation of controls or traditional internal audits (including forensic or fraud audits) is low: 42% according to a 2008 study by the Association of Certified Fraud Examiners. A continuous risk and control assurance program that includes monitoring risks, assessing and testing controls, and testing data should increase significantly the likelihood that fraud is prevented or detected on a timely basis.

On-Demand Data Mining

When potential control issues are identified or risk levels rise for unclear reasons, the auditor is likely to need additional information to determine the appropriate actions (which can range from inquiries of management to an on-site audit or even a formal investigation). The information may be obtained through “on-demand data mining” of application data or after extracting the relevant information to a data warehouse. As with continuous data mining, the data warehouse could be an existing corporate data warehouse or one developed for the continuous assurance program.

The Monitoring of Key Performance Indicators

KPIs are established so that management at each level can monitor the business. They provide the information necessary to understand the success or failure of initiatives and programs and to take action as appropriate.

KPIs are important sources of information for auditors as well. A failure to achieve goals and objectives, or financial and operation targets, is often a strong indicator that related risks are not effectively managed or related internal controls are ineffective.

The monitoring of KPIs should be a key component of the continuous risk and control assurance program, and its results considered together with those of the continuous risk-monitoring program. The internal audit team should give strong consideration to periodic reviews or audits of the KPI processes to ensure that the KPIs can be relied upon by management and used for the continuous assurance program.
Continuous Reporting

Continuous assurance is not provided without communication to the key stakeholders. They will have peace of mind and “sleep through the storm” only if they have received assurance that the more significant risks are managed and related controls are operating effectively.

In the traditional world of internal auditing, reports are provided at the conclusion of each audit project. In addition, many leading internal audit departments provide annual assessments of the overall condition of the organization’s risk management processes and systems of internal controls. When internal audit functions evolve and provide continuous risk and control assurance, these periodic communications have to be replaced by more current, continuous communications.

Each stakeholder’s needs must be considered when developing and providing continuous risk and control assurance information. Some may be satisfied with occasional updates that focus on exceptions – members of the board of directors, for example. Others will prefer more detailed information, with an emphasis on risks and controls relevant to their specific areas of responsibility.

If the organization has a risk management organization in place, separate from internal auditing, then both organizations should work together to present a single source of truth about the health of risk management and related controls. There is no value when the two organizations provide different assessments or assessments in different forms that serve only to confuse.

Each organization will develop the communication vehicles that best suit their culture, their mode of operation, and the needs of each stakeholder. Some may decide to use dashboards for each high-level risk area, with drill-down features allowing them to see the underlying health of risk management and related controls in detail. Others may want much more detailed reports or have totally separate reporting for each consumer of the information – for example, separate reports for the board, CEO, CFO, chief risk officer, head of environmental compliance, head of logistics, and so on. However, it is critical that all the information be consistent at all times.
The continuous risk and control assurance model will enable the internal audit function at any organization to provide more valuable, effective assurance services to their stakeholders at board and management levels. Traditional, periodic assurance engagements of relatively narrow and shallow focus will be replaced by a continuous assurance program with broader and deeper insight into the health of risk management and related controls.

One question each organization will need to address is which monitoring and auditing activities will be performed by management and which will be performed by the internal audit team. In fact, writers on the topic of continuous auditing have differentiated continuous auditing and continuous monitoring only by the function responsible for the activities: continuous monitoring is performed by management and continuous auditing by internal audit departments. There may be little or no difference in the tools and techniques used.

We do not take a position in this document on where the division of duties should be. That should depend on the following:

- The culture and organizational structure of each entity (factors to consider include whether there are multiple compliance or internal control functions and whether management, the internal audit team, or a combination of the two is expected to monitor controls)
- The maturity of the risk management process (such as whether there is a separate risk function with resources to monitor risks and report on the health of risk management and related controls)
- The efficiency of the entity’s applications (such as the ease with which monitoring can be built into the daily process of each line of business)
When management performs continuous assurance activities, internal auditors will have to determine what procedures they will follow to obtain a reasonable level of assurance that the monitoring performed by management is consistent and effective. The auditors will not be able to provide objective and independent assurance on risk and controls unless they are comfortable with management’s continuous monitoring activities.

There will certainly be an initial investment required of time and resources, and maintenance will be essential to ensure that the continuous assurance program continues to be effective in addressing current risks and related controls. But the continuous assurance program should be more efficient and consume fewer resources than a traditional, comprehensive assurance program. This represents further opportunities for the leading-edge internal audit department, as follows:

- Resources can be assigned to monitor and respond to changes in the health of risk management and related controls, ensuring prompt action by management to mitigate any adverse effects.
- Internal auditors can turn their attention to emerging risk areas, where the business is changing. For example, internal audit will have the resources to participate proactively to ensure that risk management and control aspects of new processes and systems are part of the initial design and implementation, rather than afterthoughts. The same approach can be taken to internal audit involvement in merger and acquisition activities, changes in business plans, development of new products, and so forth. Each time, the internal audit team assumes an advisory role. It ensures that risks associated with the business change are considered and responses are developed, that appropriate risk monitoring will be in place, and that all required key controls are identified early and implemented effectively.
- Additional resources are likely to be available for value-added consulting activities that focus not only on whether governance, risk management, and internal control processes are effective but also on whether they are efficient.
- In the traditional internal audit model, significant resources may be spent developing audit programs and building working papers. When technology is used to enable continuous testing, it generally includes the ability to maintain a record of the tests performed and results obtained – including workflow for managing and resolving exceptions. For example, if an automated data mining routine identifies an anomaly, where an individual has been granted access to finished goods inventory but his or her job description (according to the HR system) does not indicate that there is a business need for the access, then an alert is sent to the auditor. Workflow associated with that alert can capture the auditor’s resolution of the issue. If management action is required to address a problem (such as to remove the access), then that is recorded in the system, routed to management for action, reported as open until completed, and the resolution is captured and retained.

The level and type of day-to-day work performed by internal auditors will change, and it will involve more and deeper discussions with management about the business, its risks, and controls. Auditors will be recognized as value-adding contributors, so that both the work will be more interesting and the recognition for their efforts will be much greater.
Other Resources

Material referenced in this document includes:

- Institute of Internal Auditors:
  - Global Technology Audit Guide: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment
  - International Standards for the Professional Practice of Internal Auditing
  - GAIT for IT and Business Risk

- Institute of Internal Auditors, Association of Certified Fraud Examiners, and the American Institute of Certified Public Accountants:
  - Managing the Business Risk of Fraud

- KPMG:
  - Continuous Auditing/Continuous Monitoring: Using Technology to Drive Value by Managing Risk and Improving Performance

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO):
  - Enterprise Risk Management Framework
  - Guidance on Monitoring Internal Control Systems

- The Institute of Internal Auditors – Australia and Standards Australia:
  - Delivering assurance based on AS/NZS 4360:2004 Risk Management

- Standards Australia and Standards New Zealand:
  - AS/NZS 4360:2004 Risk Management

- PricewaterhouseCoopers:
  - Internal Audit 2012: A study examining the future of internal auditing and the potential decline of a controls-centric approach
1. The continuous testing has several forms, depending on what is most efficient and effective, considering the level of risk. It includes:
   - Automated tests of every transaction, where exceptions are reported through alerts (for instance, invoices approved for payment by individuals without that authority, or with conflicting responsibilities)
   - Semiautomated testing, where specific types of activity are reported periodically for review to determine whether there are reasonable explanations or they are exceptions (for example, changes to the configuration of an SAP automated control)
   - In a few cases, reliance on management’s continuous monitoring of the controls
     - Generally, an automated request is sent to management asking that it confirm that the control is operating properly. On a periodic basis, depending on the level of risk, we will perform audit procedures to confirm management’s self-assessment.

2. This is another result and benefit from the GRC convergence program (discussed in “The Journey from Traditional Auditing” section of this document). The risk level for inventory theft is changed if there is a poor security inspection. Internal audit may respond with unannounced attendance at the next routine physical inventory.

3. Edgar explains: “One of our strategies for continuous assurance is that we monitor the business results for indicators of a change in risk levels. In addition to attending management operational and financial review meetings with the major subsidiaries, we download the detailed financial results each month into our internal audit data warehouse. Our business intelligence software provides us with regular reports of unusual variances and trends. For example:
   - An increase in sales in an emerging nation might indicate increased risks to revenue recognition and ethics compliance. This information is fed into the risk assessment and the underlying analysis retained in the data warehouse.
   - A concentration of purchases through a single vendor might be a fraud indicator.
   - A large number of credit memos at the beginning of the quarter could indicate ‘channel stuffing’ and increased revenue recognition risk.
   - An increase in key inventory metrics (especially the number of days’ sales we held in any inventory category) might indicate an efficiency issue: in procurement, manufacturing, or logistics.”

4. “Although it did not come up during our work on this incident, we found out later that the CFO’s daily dashboard reflected the potential loss situation and he had called the local controller and the corporate risk manager. Because we were working together to resolve the issue and take any necessary actions, all he did was make a note and follow up at the end of the month. He told me in our next meeting how pleased he was with the added value our continuous assurance program, coupled with our problem-solving approach, provided him and the rest of the executive team. The CFO made a point of informing the audit committee.”

5. Protiviti Inc., a firm specializing in internal audit, risk, and business consulting, published the 2009 edition of its Internal Audit Capabilities and Needs Survey summarizing responses from more than 1,000 internal auditors. These auditors cited continuous auditing, computer-assisted audits techniques (CAATS), data analysis tools (statistical analysis), and data analysis tools (data manipulation) as the areas where they needed the greatest improvement, regardless of their level of competency in those areas. Further, chief audit executives participating in the survey agreed that they too most wanted to improve in those areas, compared to more than 40 other topical choices covering internal audit process knowledge.
Robert Hirth, executive vice president and global leader of Protiviti’s internal audit practice stated, “Continuous auditing, CAATS, and automated data analysis are all just the kind of ‘looking through the front windshield rather than the rearview mirror’ techniques internal auditors need in order to be relevant and add value in the eyes of their stakeholders as well as to stay up with the business itself and effectively help their organizations manage risk, which by its very definition is future oriented.”

6. The IIA, in its global technology audit guide, *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*, defines continuous auditing as “a method used to perform control and risk assessments automatically [we disagree with the “automatically” limitation, as noted in this document] on a more frequent basis.” It describes continuous monitoring as “the processes that management puts in place to ensure that the policies, procedures, and business processes are operating effectively.” KPMG LLP’s 2008 publication *Continuous Auditing/Continuous Monitoring: Using Technology to Drive Value by Managing Risk and Improving Performance* describes continuous auditing as “the collection of audit evidence and indicators by an internal auditor on information technology (IT) systems, processes, transactions, and controls on a frequent or continuous basis throughout a period.”

KPMG defines continuous monitoring as “a feedback mechanism used by management to ensure that controls operate as designed and transactions are processed as prescribed.” These definitions are expanded later in the document: “CA [continuous auditing]/CM [continuous monitoring] needs to monitor the risks that would prevent the organization from achieving its objectives.”

7. The 2008 publication *Continuous Auditing/Continuous Monitoring: Using Technology to Drive Value by Managing Risk and Improving Performance* by KPMG notes that “while the definitions of CA and CM may vary across organizations and industries, the goal in pursuing these disciplines is to provide greater transparency, effectively manage risk and performance, and provide continuous assurance. Depending on an individual’s role within the organization, he or she can think of CA or CM as a lens to assess and/or monitor the effectiveness of the organization’s governance, risk, and compliance (GRC) program.”

8. Published in 2007.

9. KPMG’s 2008 publication *Continuous Auditing/Continuous Monitoring: Using Technology to Drive Value by Managing Risk and Improving Performance* comments that: “As business risks of all kinds continue to proliferate, management and internal audit departments are actively seeking...”
new ways to quickly gain access to valuable information to manage risk and improve performance. Such efforts increasingly include continuous auditing and continuous monitoring of organizational processes, systems, and controls."

It continues: "What’s more, management and internal audit efforts to adapt innovative ways of assessing and managing risk and enhancing performance are now more critical than ever. Providing senior management with a ‘post mortem’ after a problem has occurred is no longer acceptable. . . . As a result, management and internal audit teams are embracing CA and CM as important efforts that can provide efficient and continuous discipline to monitor issues on a frequent or real-time basis, resulting in risk events being addressed before issues arise."

10. The definition of internal auditing, according to the Institute of Internal Auditors, is as follows: "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

Standard 2120 provides further detail: "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes."

**Interpretation:**
"Determining whether risk management processes are effective is a judgment resulting from the internal auditor’s assessment that:

- Organizational objectives support and align with the organization’s mission;
- Significant risks are identified and assessed;
- Appropriate risk responses are selected that align risks with the organization’s risk appetite; and
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

"Risk management processes are monitored through ongoing management activities, separate evaluations, or both."

Standard 2130.A1 is important, as it indicates that the evaluation of controls should be as they relate to enterprise risks: "The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization’s governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts."

The handbook developed by IIA-Australia and Standards Australia, *Delivering assurance based on AS/NZS 4360:2004 Risk Management*, comments on the need to “focus audit and assurance activities on those risks which, if the controls were absent or had failed, would expose us to high and unacceptable consequences. In those cases assurance activity is there to provide ‘assurance’ that key controls are both adequate and effective.”

11. References to the "board" include the board itself and/or one or more of its committees, such as the audit committee, governance committee, risk committee, or similar.

12. The Committee of Sponsoring Organizations of the Treadway Commission’s (COSO’s) *Enterprise Risk Management Framework (ERM)*, published in September 2004, defined enterprise risk management as follows:
Enterprise risk management is a process, effected by an entity’s board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

13. COSO ERM defines control activities as “the policies and procedures that help ensure risk responses are properly executed. Control activities occur throughout the organization, at all levels and in all functions. Control activities are part of the process by which an enterprise strives to achieve its business objectives.”

14. Internal auditors use factors such as the results of prior audits, the status of open audit findings, and the time since the last audit in addition to operational factors typically included in management’s assessment of risk (such as the volume of business and related trends). We believe these factors should be included in management’s risk assessment process as well.

15. See note 10.

16. The IIA standards define control processes as “the policies, procedures, and activities that are part of a control framework, designed to ensure that risks are contained within the risk tolerances established by the risk management process.”

The concept of key controls has been described in other IIA documents. For example:

- The IIA-Australia and Standards Australia Handbook, Delivering assurance based on AS/NZS 4360:2004 Risk Management, defines key control as “controls or groups of controls that are believed to be maintaining an otherwise intolerable risk at a tolerable level.” The handbook continues to discuss control adequacy: “Adequacy of risk management, control, and governance processes is present if management has planned and designed them in a manner that provides reasonable assurance that the organization’s objectives and goals will be achieved efficiently and economically.”

- Similarly, the IIA’s GAIT-R publication, GAIT for Business and IT Risk, says key controls “relied on to ensure failures in achieving business objectives will be either prevented or detected on a timely basis.”

17. This document does not include details on how to identify all the key controls required to address a business risk. There are other publications that provide such guidance, including the IIA’s GAIT for IT and Business Risk.
available from the technology section of its Web site at www.theiia.org.


Principle 2 in that document states: "Fraud risk exposure should be assessed periodically by the organization to identify specific potential schemes and events that the organization needs to mitigate."

Principle 4 addresses fraud detection: "Detection techniques should be established to uncover fraud events when preventive measures fail or unmitigated risks are realized."

19. While management as a whole is responsible for the system of internal control, when it comes to monitoring the system of internal control, the board and management may rely on a combination of management and internal audit-monitoring procedures. COSO’s 2009 publication Guidance on Monitoring Internal Control Systems explains:

“Organizations may select from a wide variety of monitoring procedures, including but not limited to:
- Periodic evaluation and testing of controls by internal audit,
- Continuous monitoring programs built into information systems,
- Analysis of, and appropriate follow-up on, operating reports or metrics that might identify anomalies indicative of a control failure,
- Supervisory reviews of controls, such as reconciliation reviews as a normal part of processing,
- Self-assessments by boards and management regarding the tone they set in the organization and the effectiveness of their oversight functions,
- Audit committee inquiries of internal and external auditors, and
- Quality assurance reviews of the internal audit department.”

20. The IIA’s Global Technology Audit Guide (GTAG) on Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment defines continuous auditing and continuous monitoring as follows: "Continuous auditing is a method used [by auditors] to perform control and risk assessments automatically on a more frequent basis.

“Continuous monitoring encompasses the processes that management puts in place to ensure that the policies, procedures, and business processes are operating effectively.”

The GTAG continues: "Many of the techniques of continuous monitoring of controls by management are similar to those that may be performed in continuous auditing by internal auditors.

"Management’s use of continuous monitoring procedures, in conjunction with continuous auditing performed by internal auditors, will satisfy the demands for assurance that control procedures are effective and that the information produced for decision making is both relevant and reliable."
We at SAP would like to express our appreciation to the following individuals (and to those who prefer to remain anonymous), who contributed with their ideas and constructive criticism as the continuous risk and control assurance model was being developed:

Professor Andrew Chambers, Management Audit LLP
David Coderre, CAATS
Mark Gosling, PricewaterhouseCoopers LLP
Roger Herd, Western Refining Inc.
Ed Hill, Protiviti
Robert Hirth, Protiviti
Suzana Keller, Coca-Cola Enterprises Inc.
Marty Patton, Cypress Semiconductor
Michael Rasmussen, Corporate Integrity
James Roth, Audit Trends
Dr. Sri Ramamoorti, Grant Thornton LLP
Miklos A. Vasarhelyi, Rutgers University
Louis Vaurs, Institut de l’Audit Interne
Curt Verschoor, DePaul University
Don Warren, DePaul University
Manfred Wolf, SAP AG
David Zechnich, Deloitte & Touche LLP