



Continuous Controls Monitoring: Where To Start?

Wednesday, November 09, 2005

William McNeill

As accelerated filers complete Year 2 activities to comply with the Sarbanes-Oxley Act (SOX), companies are investigating ways to automate activities to make compliance repeatable, sustainable, and cost-effective. For many, including those organizations still facing down first-year activities, Continuous Controls Monitoring (CCM) is a next logical step to take a large chunk of human effort out of the ongoing process. At this year's **OpenPages** user conference in Boston, a panel of CCM vendors, moderated by AMR Research's John Hagerty, addressed five important questions companies want answered about when, where, and how to deploy CCM technologies effectively. Panel members included John Verver, vice president of professional services at **ACL Services**; Arthur Stewart, principal at **Greenlight Technologies**; Patrick Taylor, CEO of **Oversight Systems**; and Dr. Mark Feldman, senior vice president of business development at **Virsa Systems**.

Q. What is the difference between controls automation and the automation of the testing of those controls, and where does CCM fit in?

Controls automation reflects programmatic logic that is meant to prevent, detect, and/or remediate transaction errors or deliberate fraud, either in real time or near real time.

Automating the testing of those controls confirms whether the control itself is even effective in preventing errors or fraud from occurring. In theory, you can completely automate activities that are wholly ineffective. But without testing, how would you know?

Let's look at an example. Many companies currently use three-way matching in voucher processing. This process ensures that the original purchase order, supplier's invoice, and purchase order receipt for the received items are all in agreement before a payment to the supplier can be generated.

- If a person does the three-way match by hand, that's a manual control.
- If the company sets up its Enterprise Resource Planning (ERP) system to do the three-way match automatically, that's controls automation.
- If the process owner periodically tests the control (verifies the three-way match is being done every time correctly), that's a manual test.
- But if this periodic test is performed by a system or process that monitors the three-way match control automatically, records the results of tests electronically, and issues alerts to the process owner if something is outside expected results, that's automation of the testing of the control.

CCM performs mostly the latter functions, such as the testing of controls effectiveness. In testing controls, CCM software can help you detect weaknesses in your controls structure, flaws with your existing process, or both. In addition to supporting compliance, it can also lead to better transaction quality by pointing out holes in processes you thought were closed. For detailed profiles on CCM vendors, see the *AMR Research Report "Profiles in Compliance,"* September 2005.

Q. Where do I start?

With CCM, a good place to start is in areas of high exposure where you know or suspect violations are occurring. After you install the software, run it and see what the testing process comes up with.

- Are there a disproportionately high number of errors in a particular process?
- Are there any patterns that have emerged that can pinpoint source(s) of errors?

Another strategy: start from the outside and work your way back in. For example, examine your customer- or supplier-facing processes first, and then examine your internal processes that support them. Spotting a fraudulent invoice from a vendor or sniffing out duplicate payments is significantly more straightforward and can have a quicker Return on Investment (ROI), especially when compared to an internal process of managing security settings in an ERP system. Much of the security work in support of segregation of duties requirements requires companies to untangle some snarly situations. Examining these outward-facing processes and transactions first can point to basic flaws in your internal processes. It's tough to see where the security violations are happening in your ERP system if you can't see what results they are producing or allowing.

Q. Where is the ROI for CCM?

Continuous controls monitoring software provides two kinds of ROI:

- **Soft dollars** come from time saved manually testing controls. Once the software is up and running, companies spend fewer hours testing for their internal audit.

- **Hard dollars** come when companies find errors or fraud and recoup money. In turn, the software can quickly pay for itself, and this helps buyers create a strong business case for implementing the software in even more areas of the business, even outside traditional financial processes.

Each panel participant presented several good case studies on how companies recouped the cost of the software quickly, sometimes within weeks, usually within months. ACL Services presented a particularly compelling example: a supplier was billing two divisions of the same company, one in the United States and the other in Mexico. Because the two divisions' ERP systems didn't talk to each other, they both paid the supplier because there was no way to check across divisions. The company implemented the ACL software and within minutes found the duplicate payments that nearly paid for the ACL software immediately. That's a textbook definition of quick ROI.

Q. If a company implements controls that are so effective, why do they need to test the controls?

The simple answer: proof. Internal and external auditors require proof that the controls are in place and working. SOX rulings not only require that each company has controls in place for its financial reporting processes, but requires that company executives acknowledge that the controls are effective. The best way to prove they are effective is to test them. Company executives aren't the only ones with their feet to the fire. External auditors are being held to the same standards, and as much as they would like to take a company's word for it, they would rather see some testing going on.

Q. Will CCM software eventually replace auditors?

There was general and emphatic agreement that this class of software would not replace auditors. Although it obviously benefits CCM vendors to say this, AMR Research agrees. CCM products remove some of the heavy lifting and much of the drudgery of auditing tasks. It allows auditors to flex their brain muscle and engage in the higher value work. Arthur Stewart from Greenlight Technologies added that auditors with ERP backgrounds are in especially high demand right now. Although we wouldn't necessarily agree with his statement that "There are never enough auditors," we understand the point.

Conclusion: The next step for many companies in their SOX compliance efforts is automation: of key controls and the testing of the key controls. At this conference, many companies were ready to explore this path, as evidenced by the depth and breadth of questions. Continuous controls monitoring can deliver benefits in time and money and should be considered by any company looking for the next step (after documentation) in their SOX compliance efforts.