

COMPLIANCE WEEK

August 15, 2007



 PRINTABLE VERSION

The Secret Life of Application Controls

By Todd Neff — August 14, 2007

Viruses. Worms. Trojans. Denial-of-service attacks. IT security professionals have long wrestled with these and many other external threats, and a bustling industry has sprung up to fend off the pests.

Such risks and others posed by those aiming to compromise corporate IT systems and steal data have garnered nearly all the public attention. And from a compliance perspective, protecting the ramparts against IT security threats is crucial. But it's only part of a larger story that includes a much less sexy chapter on application controls.

A recent piece of guidance from the Institute of Internal Auditors, "Auditing Application Controls," may not make headlines, but the eighth of the organization's Global Technology Audit Guides explains what application controls are and shows auditors how to handle them. Success has more to do with hard work than a magic bullet from a software vendor.

First, some semantics. Say "application controls" to an IT security expert and visions of SQL injections, phishing and buffer-overflow exploitation dance in his head. Alan Paller, director of research at the SANS Institute, which specializes in information security training and certification, says IT security folk associate application controls with security, the virtual fence your company erects between your local network and the big bad Internet.

Phishing and the like are designed to breach that perimeter, and such threats are common and real. But they fall under what the IIA authors call "IT general controls," or ITGCs, which are better known as general computer controls, or GCCs. Strong GCCs are a condition of and precursor to good application controls.

Application controls, in the IIA's view, specifically entail making sure a company's IT applications work as the organization believes they should. Application controls include such things as checking that sales orders are within customer credit limits, ensuring proper financial calculations, monitoring for proper segregation of duties, and ensuring a three-way match between the purchase order, receiver, and vendor invoice.



Hunt

"With SOX, there's no question. If you're publicly held, you're paying much more attention to application controls than you ever have," says Steve Hunt, an executive at the consulting firm Enterprise Controls Consulting LP, who wrote the IIA report with Christine Bellino of consulting firm Jefferson Wells.

Karine Wegrzynowicz, an internal audit director specializing in IT audit at LaFarge North America, says application controls are familiar to companies facing regulatory mandates of HIPAA, Sarbanes-Oxley, or rules specific to the financial-services sector such as the Gramm-Leach-Bliley Act. But, she adds, "In some organizations ... I don't think they are fully embraced or understood as one of the key elements of an information security or control program."

Maria Castellanos, vice president of internal audit at AXA Equitable Life Insurance, says her company was concerned with application controls long before Sarbanes-Oxley made them a compliance priority. SOX has prompted AXA Equitable to print out documentation related to application controls for external auditors to review. But, she says, many other, non-SOX forces drive her to pay attention to application controls anyway.

Sarbanes-Oxley "only impacts the systems related to financial reporting; Sarbanes is not holistic," she says. "Business continuity planning is not part of Sarbanes. I care about all these other systems." AXA Equitable establishes its application controls from a top down, risk-based perspective, according to Castellanos, starting with an understanding of how the business works and what software underpins various business processes. They prioritize application controls based on business risk—for example, dollar value—as well as on compliance and

privacy risks and other regulatory considerations.

The controls often use common sense. An application shouldn't let a customer with a \$20,000 balance withdraw \$50,000, for example. AXA Equitable monitors them continuously, as well. For example, Castellanos says, her team recently questioned the quality of data coming from a front-end application that had been designed for speed, but lacked certain desirable ways to validate inputs.

At LaFarge, Wegrzynowicz rates applications on what she calls the "three pillars of confidentiality, integrity, and availability." She uses a point system or high-medium-low rating scheme. "To do this, there must be an understanding of core business process flow from end to end, to know the input and outputs of each application and what processing occurs," Wegrzynowicz says. "Based on the point rating, a risk-based approach can determine the frequency and depth of application audits or reviews."

All Together Now

Because applications directly support business processes, cooperation between business units and IT is particularly important. "It's the age-old thing. Business says it's IT's job. IT says it's business's job," Castellanos says. "It's both."

Lily Bi, the Institute of Internal Auditors' manager of technology practices, says internal auditors can help bridge the business-IT gap.



Bi

"Senior managers leave the job to IT, but IT may not understand the business aspects," Bi explains. A tech-savvy internal auditor can help the two sides understand their needs. And that need is likely to grow only more acute with the new Auditing Standard No. 5 from the Public Company Accounting Oversight Board, which stresses the advantages of automated application controls.

"Entirely automated application controls are generally not subject to breakdowns due to human failure," the standard reads. As long as general computer controls do their job with respect to program changes, user access and the like, "the auditor may conclude that the automated control continues to be effective without repeating the prior years' specific tests of the automated application control." That assumes, of course, that the application program, related files, tables, data and parameters—not to mention the application control itself—have not changed.

For businesses running on enterprise resource planning software such as SAP and Oracle Applications, configuring them properly is half the application-controls battle. Hunt from Enterprise Controls Consulting says consultants doing major ERP installations have neither the time nor inclination to think through the compliance or business-risk implications of configuring these Byzantine systems in subtly different ways.

"I've seen companies go live with new ERP solutions and all of a sudden they're seeing these major balances swing up out of nowhere on the balance sheet or P&L," Hunt says. "They didn't adequately focus on application controls."

SCOPING SCHEMES

Below is an excerpt of the recent IIA guidance on application controls, elaborating two methods of scoping controls for audit.

Business Process Method

The business process scoping method is a top-down review approach used to evaluate the application controls present in all the systems that support a particular business process. Over the past several years, this method has grown in importance as the most common and widely accepted scoping methodology. This is primarily due to an increase in ERP transactional application use and a reduction in stand-alone, "best of breed" applications.

When using the business process method in the non-ERP world, internal auditors should include within the review's scope all of the applications used by the company that are involved in the business process under review because they are generally stand-alone systems. In other words, the auditor needs to include within the review's scope the separate applications that make up the different components of the business process cycle. The auditor can then identify the inbound and outbound interfaces within the application under review and complete the scoping activity.

Using the business process method to scope the review of application controls is different with integrated applications such as an ERP system because business processes cut across multiple modules. For example, consider the procurement to payment business process. In an ERP environment, this process generally consists of the procurement, inventory management, general ledger, and accounts payable modules or subapplications within the ERP system. Therefore, it is important to have a thorough understanding of the modules that comprise the business process and how the data is managed and flows from one module to the other.

Single Application Method

The single application scoping method is used when the auditor wants to review the application controls within a single application or module as opposed to taking a business process scoping approach. As discussed earlier, this is the most effective scoping method in a non-ERP or non-integrated environment because the auditor can more easily "draw a box" around the application (i.e., include the application within scope). In other words, the auditor can identify the inbound data inputs and outputs because data and related processing rules are contained and used only for one application.

However, in an ERP or integrated environment, this method is not desirable. Although it may appear to be fairly easy to draw a box around the module of an ERP or integrated transactional system, the reality is that this activity can be quite difficult. This is because there can be multiple data feeds into and out of any given module, and attempting to identify them could prove to be an exercise in futility. Therefore, using the module approach is likely to lead to an inadequate review; using the business process method is a more effective scoping method in an ERP or integrated environment.