



## Solving the Audit Gap

**When it comes to keeping IT-related control deficiencies to a minimum, it's more important to improve communication than it is to improve your technology.**

[Jabulani Leffall, CFO.com](#)

October 02, 2006

A piece of technology that's probably already available in your office can help solve many of the IT-related deficiencies that crop up in internal control audits. What is it? The electric elevator, first built by Werner von Siemens in 1880.

In all too many companies, before, during and after an audit, finance executives simply don't go down to the data center, while IT executives don't come upstairs to the finance department, says Michael Cangemi, an IT governance consultant who has been both a CFO and CIO at various times in his career.

In the first round of internal control audits performed after the Sarbanes-Oxley Act passed, control deficiencies related to IT proved to be a major irritant to finance executives. In one infamous [example](#), Santa Fe, New Mexico-based Thornburg Mortgage complained in a letter to the SEC that it had installed up-to-date antivirus software to protect its computer systems — but was tagged with a deficiency by auditors because there was no paper trail documenting the software installation.

Frustration over such incidents boiled over during a 2005 roundtable on Sarbox section 404 sponsored by the Securities and Exchange Commission. Representatives of several major companies complained bitterly about the way audit firms evaluated IT control weaknesses, and argued that weaknesses might not even affect financial reporting.

Pronouncements issued since by both the SEC and PCAOB stressing the need for a risk-based assessment may reduce the number of IT audit horror stories, but the fact remains that audits of information technology are a challenge for finance professionals who rely heavily on IT systems, but don't necessarily understand how they work. At the same time, regulation has now saddled IT professionals at most public companies with as many as three different types of audits, and not everyone in IT may understand the difference.

Many IT departments perform audits that focus not on financial issues, but on the company's general computer controls, or GCCs. (For a description of such IT audits, see ["You Bought It, Now Audit."](#)) Meanwhile, Sarbanes-Oxley section 404 requires testing of internal controls over financial reporting, which, of course, often reside on computer systems. That means the IT department is typically involved in both a readiness assessment — an internal audit that is part of getting ready for the actual 404 audit — and the attestation, or external, audit.

Cangemi, who is also a former president of the Information Systems Audit and Control Association and author of *Managing the Audit Function*, believes that the CFO should take a strong role in all three types of audits because "he or she is the one cutting the checks and the one ultimately responsible and accountable for the whole audit, part of which has consultants taking a look at the inner-sanctum of IT."

That, however, is not often the case. "All the controls are related," says Robert Greene, IT Audit Practice Leader for Haskell & White LLP. "But the CFO often knows little about IT controls or how they function or may be tailored to best address the corporate needs. There are also manual controls that are initiated in the finance department that are not addressed or understood by the IT team."

For example, sales transactions from retail stores upload to the server at company headquarters in the form of "batches" of data. A frequently-applied control objective for the IT operations section of GCCs calls for the batches to be conveyed to the system in an efficient and expedient manner. Indeed, this is a practice called for by COBIT (Control Objectives for Information and Related Technology), a technology-governance model now published by the IT Governance Institute, and [used by about a third of CFOs](#) as a control framework, according to a *CFO* survey done in January.

To ferret out exceptions and/or duplicated data, the IT department typically conducts a periodic review of a system-generated activity log, yet doesn't necessarily share that information with the finance department. At the same time, it's not unusual for a finance department to have a related business process or manual control such as the review and approval of a revenue allocation spreadsheet based on the batches of info. The IT department often doesn't participate in this exercise.

The risk, obviously, is that if batches aren't loading correctly, the spreadsheet is useless and erroneous numbers could filter through to the general ledger, affecting the validity and timeliness of financial information during the period or quarter close. Simply improving communication so that finance is aware of the system activity log and IT knows about the spreadsheet can help head off problems before they find their way into financial statements.

But a gap such as this can't be filled if the two sides don't talk regularly, notes John Stevenson, a past president of the Society of Information Management and a former CIO at Sharp Electronics, America. "Sometimes company leadership is not proactively engaged in fixing leaks," Stevenson said. Likewise, technology chiefs are concerned about making sure data is flowing — they don't typically dwell on how, and in what context, it is analyzed by finance. Yet, this can lead to deficiencies when the controls don't pass muster in the eyes of an auditor.

Robert Young, CFO of Teradata, a division of NCR Corporation, says he tries to keep himself informed of developments in IT "as often as humanly possible."

"If everyone understands the audit plan from finance to tech — from top to bottom — the holes can be plugged everyday and not just when it's time for the audit," he added.

Finance executives, observers say, should develop an overall corporate audit and controls planning group, as well as an IT steering committee that includes senior managers from all departments. This approach can make audits run smoother or at least get all sides talking.

"If the CFO and CIO are either clueless or out of sync with each other, the company is usually out of harmony with itself and by extension customers and regulators," says [Jerry L. Mills, founder and chief executive of B2B CFO/CIO](#), a consulting company. "Run your audits this way you're losing the game before it even started."