

Beyond Checklists:

A Socratic Approach to Building a Sustainable Change Auditing Practice

By Dwayne Melançon

Issues related to IT change control rarely have been as important as they are now. Chief audit executives (CAEs) are being held accountable by audit committees and are expected to comply with regulations such as the US Sarbanes-Oxley Act of 2002, section 404. Business professionals must not overlook the fundamental reason for auditing change, which happens to be the same reason anything is audited: to protect the business from risk. At the end of the day, that is the job of an auditor.

Any IT risk can be exacerbated by ineffective IT change management. Recent research¹ has demonstrated that poor IT change and patch management increases downtime and costs. Industry analysts IDC and Gartner Group estimate that as much as 70 to 80 percent of all changes resulting in downtime or reduced operational capabilities are, in fact, initiated by people within the organization—and most of those changes are accidental or unintentional.

Further, there are many prominent examples of the problem. CNET News reported that in 2001, a “router configuration error” at Microsoft interrupted service to *Microsoft.com*, *MSN.com*, *Expedia.com* and others. Full service was not restored until 22 hours later.² In 2004, the *Globe and Mail* reported on a relatively minor software change at the Royal Bank of Canada (RBC) that resulted in “10 million RBC customers who couldn’t be sure of their account balances for days at a time and untold number of people left waiting for pay deposits and other transfers.”³

Sarbanes-Oxley increases accountability for organizations and individual management stakeholders by requiring executive management to understand and sign off on the controls over financial reporting—including IT controls. Without effective IT change management, it is difficult to see how management can meet the Act’s requirements and affirm the integrity of financial statements.

For auditors in today’s highly regulated environment, having the knowledge to effectively challenge IT management is not only useful, but essential.

However, IT auditors often have trouble determining whether an organization’s IT change management processes are effective. This is a result of several challenges facing auditors, including:

- Much of the audit guidance is in the form of checklists, and understanding which control activities are most important is often lost.
- Much of the written guidance predates new research that can help auditors focus on the right areas. This research shows that certain change control activities are not only foundational

to reducing business risk, but also provide substantial business effectiveness and efficiency benefits.

- Perhaps most significantly, many auditors are not adequately equipped to effectively challenge IT management, and they are sometimes hoodwinked by the answers they receive around change control issues.

With year two of Sarbanes-Oxley, compliance has undoubtedly become a corporate imperative, demanding ongoing resources. This article seeks to assist internal auditors in establishing a sustainable change management auditing practice. The end goal is to encourage IT organizations to operate in a way that protects their businesses from risk and helps make compliance a driver of repeatable best practices and business value.

Learning From the High Performers

Over the past five years there has been significant progress in establishing a causal relationship between key IT controls and IT effectiveness. This research was originally begun by the IT Process Institute (ITPI), a nonprofit entity whose mission is to study IT organizations and evangelize best-known methods.

As this research progressed, ITPI was joined by Carnegie Mellon’s Software Engineering Institute, ISACA, the Institute of Internal Auditors and a number of other organizations.

Their research found that high performers spent half as much time on Sarbanes-Oxley compliance efforts than their industry counterparts because they already had controls and processes in place. What set these high performers apart was that access and change controls were central to IT infrastructure management. In other words, change management and change control were built into the very culture of IT management.

Many of ITPI’s findings are codified in its publication, *The Visible Ops Handbook*. The findings from this research are a primary influence on the information presented in this article.

Establishing a Sustainable Change Audit Practice

A sustainable change audit practice can be built by first determining the effectiveness of a change management system by testing three primary areas referred to as the three Cs of change management: culture, controls and credibility (3Cs).

The framework provided by the 3Cs allows auditors to ask open-ended questions that will enable them to apply their auditing “detective skills” to auditing change management, even if they feel at a disadvantage due to a lack of technical knowledge.

*Change management
and change control
were built into the
very culture of
IT management.*

Culture

Studies of high performers found that a culture of change management has to exist to sustain compliance over time.⁴

Testing for Culture

The tests for culture center on questions and indicators that reveal an organization's attitude toward change. Some key aspects of culture are:

- **Tone at the top**—It is important to probe for clear, consistent communication from top management in setting the expectation that change management must be followed for the organization's success.
- **Accountability with consequences**—Policies are meaningless unless they are enforced. It is necessary to test for proof that there are consequences for violating policies.
- **Causality and management by fact**—A “culture of causality” means that there is a focus on analyzing the impact of IT changes before and after they occur. Such analysis should focus on predicting the impact of changes to enable mitigation of risk, as well as postincident analysis to learn from failed or improperly managed change. This enables organizations to systematically assign risk ratings to changes based on historical data. Since not all changes are created equal, risk ratings allow organizations to give greater scrutiny to high-risk changes.
- **Collaboration and communication**—High-performing organizations have processes that promote making changes “in plain sight” so all stakeholders and constituents have the opportunity to see, anticipate and provide input on changes before they occur. This enables proactive mitigation of risk and serves to prevent “change drive-bys” in which one group is surprised or impacted by a change initiated by another group.
- **Emphasis on people, processes and technology**—High performers understand that there is no silver bullet technical solution to a complex process such as change management. Instead, they insist on a unified program that requires people, processes and technology to work in concert.

Red flags to look for when testing for culture include:

- **The organization is paying “lip service” to change management.** In this case, the organization has a change management process but does not hold people accountable for violating the process (often because it cannot tell when people violate the process).
- **The same types of outages happen repeatedly.** This signifies that the organization is not learning from its past mistakes, or that it is relying on individual knowledge to run the business (vs. building an organizational play book).
- **The organization owns a lot of software programs, many of which seem to do similar things.** This is often a sign that the organization is looking for a silver bullet solution to its change management problems. It is easier to justify buying new software than it is to drive a change initiative that alters how people and processes work within the organization.

Controls

Studies of the high performers found that they achieve the highest leverage in properly implementing controls centered on change, access and accountability.⁵ Essentially, they focus on how work should be done in the organization, who is allowed to do that work, and ensuring that changes happen only within the organization's policies.

Testing for Controls

In the tests, many of the IT business risks have equivalents in the financial world. Finance has developed a set of controls to prevent fraud that are “baked in” to its systems and processes. They can be tested and verified at any time. IT controls should embody the same characteristics, such as controls that specify that:

- Preproduction staff cannot access production systems and must submit proposed changes via the change management process (preventive control)
- All changes must be reviewed and authorized by the Change Advisory Board prior to implementation (preventive control)
- Automated monitoring must be used to record all changes to production configurations (detective control)
- All independently detected changes must be reconciled with work authorizations to ensure that all changes are appropriate, documented and executed properly (preventive control)
- Exceptions must be removed from the environment and/or escalated as a security incident (corrective control)

A cue can be taken from the Big 4 accounting firms regarding emerging requirements in recent Sarbanes-Oxley audits. It is becoming increasingly common for these auditors to specify IT control objectives such as, “All change must be auditable, and unauthorized change must be investigated.”

With this in mind, the tests should consist of questions that probe for credible, demonstrable answers to the following questions:

- Can you detect all changes to your production environment? How?
- Can you produce a history of those changes?
- How do you determine whether change is unauthorized?
- How long does it take to discover unauthorized change?
- What happens when unauthorized change occurs?

- Red flags to watch for when testing controls include:
- **Inability to credibly answer questions about or demonstrate capability in a timely manner.** Unsatisfactory answers often rely on gut feelings or a time-consuming archaeology of system event logs, e-mail-based approvals and other inefficient methods.
 - **Inability to tell when change happens outside the process.** Many organizations have preventive controls (such as change management systems and policies) and corrective controls (such as provisioning systems or restoration processes), but have no detective controls. These organizations can report only on changes that go through the process; they are blind to changes outside the authorized process until an outage occurs.
 - **Organizations with weak IT controls tend to spend a high percentage of their resources on unplanned work.** This includes “firefighting,” e.g., break/fix activities, rework from failed change and responding to system outages.

Credibility

Credibility is where it all comes together. In this context, credibility is all about the quality of the answers received when testing for effective control processes. This is where the notion that “a good auditor is a thinking auditor” really rings true.

Now is when the high performers really shine. High-performing IT organizations recognize that their first responsibility is to protect the business from risk and operate in a manner that makes compliance audits a straightforward proposition.

Organizations with credibility have culture and controls in place that set clear organizational expectations for how work will be done within the company and how data will be collected and used as assets to the business. They also have a clear set of checks and balances in place to keep people true to the process, and they demonstrate that there are clear consequences for not following the rules.

Testing for Credibility

Testing for credibility involves asking questions that would be difficult to answer without effective culture and controls. For example, it entails asking for things such as:

- A change management compliance report showing total changes for a given period of time, with a breakout of authorized vs. unauthorized changes
- Statistics on—and causes of—failed changes
- History of unplanned outages and their causes
- Exception reports showing changes made outside the official change process

Some common indicators of credibility issues include:

- **A large volume of emergency changes.** Low-performing IT organizations often call unauthorized changes emergency changes as a way to get out of disciplining employees for violating prescribed processes.
- **A high number of system availability issues,** particularly unexplained outages or security incidents, calls for scrutiny
- **A high amount of unplanned work.** Unplanned work rates exceeding 20 to 25 percent typically indicate culture or control problems (high performers spend less than 5 percent of their time on unplanned work).⁶
- **Late projects, cost overruns incurred by bringing in contract resources to compensate for firefighting, and employee turnover** are indicators of systemic change management problems.

- **Inability to produce evidence to substantiate the presence of controls,** or excessively long response times when asked for proof to validate presence or effectiveness of controls

Forging Ahead Toward Ongoing Improvement

Moving beyond checklists and asking open-ended questions during an audit is an effective way to avoid being hoodwinked during IT audits. Using deductive skills enables an auditor to quickly get to the core purpose of the audit: verifying that management is taking responsibility for its control environment and that it is consistently behaving in a manner that protects the business from risk.

Change management audits should be anchored in culture, controls and credibility. IT teams should be coached on how to implement control strategies that satisfy all 3Cs. This will help create a sustainable change audit environment.

Dwayne Melançon

has served as Tripwire’s vice president of service and support since 2000. Prior to joining Tripwire, he was vice president of operations for DirectWeb Inc. Before DirectWeb, he ran pan-European support for Symantec Corporation, managed support for several of Symantec’s leading product lines, and spearheaded the development of tools and processes. Prior to joining Symantec, he spent eight years at Fifth Generation Systems Inc.

Endnotes

- ¹ Behr, Kevin; Gene Kim; George Spafford; *The Visible Ops Handbook*, Information Technology Process Institute (ITPI), 2004
- ² CNET News, “Microsoft blames technicians for massive outage,” 24 January 2001
- ³ *GlobeandMail.com*, “RBC blames human error,” 10 June 2004
- ⁴ Information Technology Process Institute (ITPI), IT Controls Benchmarking Survey
- ⁵ *Op. cit.*, Behr
- ⁶ *Ibid.*

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors’ employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors’ content.

© Copyright 2006 by ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org