

# Why Is Your IT Project Being Audited?

By Debbie Gallagher

You're the manager of a system implementation or custom development project and have just been told that the project is being audited. There's a possibility that you aren't exactly thrilled about this. After all, the project is going well, or maybe it's over and the new system is humming along just fine. A common response by IT folks who haven't been exposed much to audits is "but I didn't do anything wrong, so why am I being audited?" The purpose of this article is to provide some information on the reasons why your IT project could be audited. You'll notice that the reasons have nothing to do with *you*!

## Types of Auditors

First of all, you may have noticed by now that there are different types of auditors checking out your IT environment.

Here are some of the most common types of auditors that audit systems and IT processes in your organization every year:

- Financial statement;
- Controls certification readiness;
- Internal audit; and
- Regulatory.

The financial statement auditors are responsible for signing an opinion regarding the financial statements of your organization. Let's include here the folks who have to audit your controls for Sarbanes-Oxley, and any other internal controls audits. They will be from the same audit firm as the financial statement auditors and will generally perform one integrated audit to support both the financial statement opinion and the internal controls opinion. The systems focus of these audits is on IT processes and systems that could have an impact on the financial statements.

In preparation for the internal controls certification and audit, your organization may have hired auditors from another firm to help you get ready. They may be documenting your IT environment and providing feedback on control weaknesses, so that you can remediate prior to the controls certification audit. These auditors also will be financial-statement focused.

If your organization has an internal audit department, you will be used to seeing them almost every year. You may have also noticed that their focus is often different from that of the financial statement auditors. The internal auditors go beyond the financial statements to look at systems that affect operations, even if they have no financial statement impact. They frequently also have a mandate to verify that the organization's policies and procedures are being followed, or that value is being achieved for funds spent. The internal audit group may or may not be involved in assisting the financial statement auditors, depending on their mandate in your organization.

## Who reads the TUG magazine?

Over 5,000 IT professionals in the GTA, and across the country.

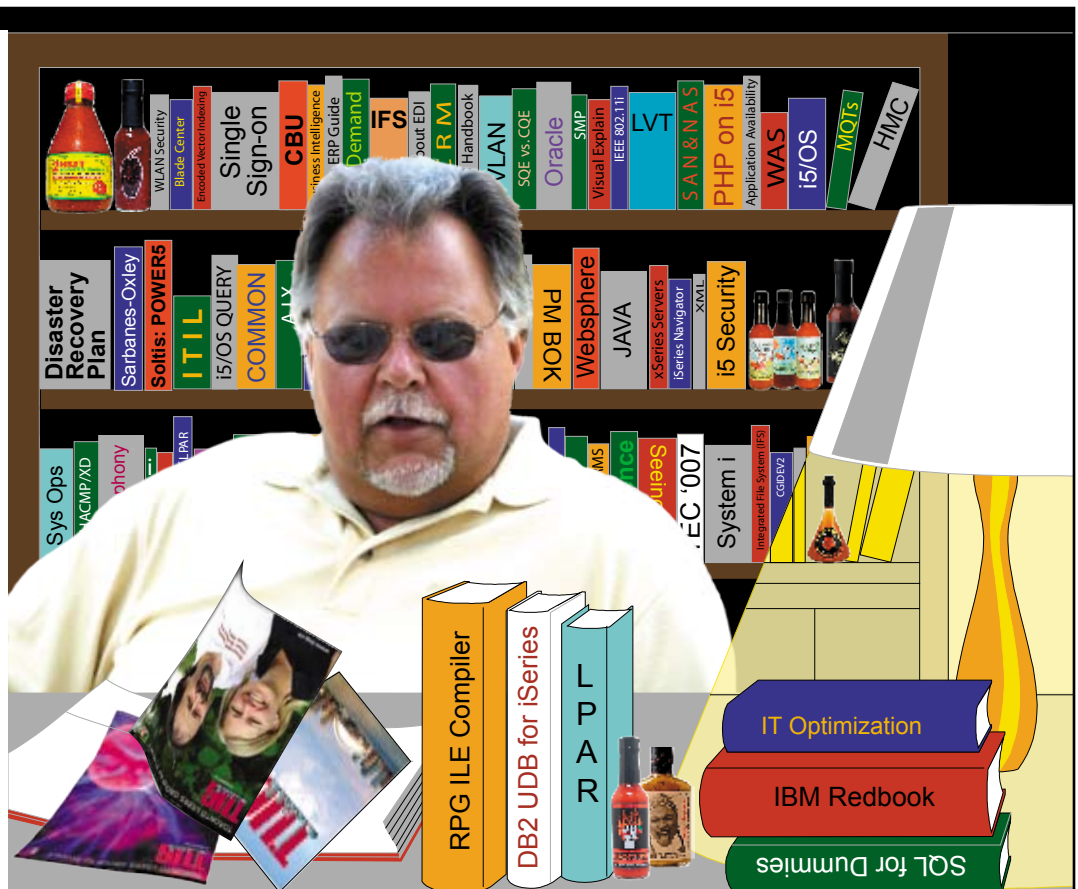
Get inside their minds...

**ADVERTISE!**  
in the TUG magazine



We are tightly focused on the midrange space.

Ron Campitelli 905-893-8217  
Wende Boddy 905-607-2546





Debbie Gallagher

Regulators frequently also perform audits. For example, if you work for a financial institution, you are subject to audits by the Office of the Superintendent of Financial Institutions. Other industries also have regulatory auditors, and if you are in one of those industries, you know that these auditors will visit you every year. Their purpose is to verify that

relevant regulations are being adhered to by the IT systems and processes in your organization.

### The Annual Audit

The financial statements for your organization rely heavily on the systems in your organization—gone are the days of binders with 14-column paper! In performing their work, the auditors also rely on reports and data from those systems. As a result, the auditors are obligated to verify the management of many aspects of your financial systems. They will check out security, networking, communications, databases, and application implementation and maintenance. They may also evaluate business continuity planning and IT strategy. Depending on a variety of factors, the financial statement auditors may look at different aspects of your systems environment each year, say networking this year and databases next year. There may also be elements, like security, that do not follow a rotation plan, so are examined each year.

The internal auditors generally have a specific set of objectives each year, based on your organization's risk assessment and audit plan. As a result, they will look at different aspects each year that they visit you. As for regulatory auditors, the work they do will depend on the type of regulatory body they are and other factors relating to the industry and regulatory environment.

### The Project Auditor

In addition to the usual array of annual auditors, you may also receive a series of visits from a specialist in IT project risk. This person or team will be hired by your project sponsor or client, who is looking for regular feedback throughout the project, so that risks can be managed timely. The hiring of this additional audit team is likely to occur in industries where there are a number of stakeholders to satisfy, or when the project is very large and high risk. The project risk audit team is likely to examine your project more frequently and in more detail than the various types of annual auditors.

### The Project Audit

As part of the annual audit planning process, the audit team evaluates your organization and the risks in your environment. In this risk assessment, they are considering *inherent* risk, which is the level of risk that exists if there are no controls in your environment. So, for example, what would be the impact if everyone in the

organization could sign a cheque, or if no one tested that new application system?

The audit team will then focus their work on the areas identified as highest risk. Although the areas of greatest risk vary by type of industry, a new system nearly always has a high probability of being identified as a medium or high risk. As a result, your IT project has a high likelihood of being audited, by the financial statement and controls certification auditors, the certification readiness team, the internal audit team, regulatory auditors, and maybe also project risk auditors. As noted earlier, the various auditors have different focus areas and objectives. As a result, you may find that your project is audited several times.

### It's Not About You

So, as you can see, the project audit isn't about you at all. It's driven by the audit team's assessment of risk. In the next article, I'll provide some information on what the key areas of focus are likely to be on your IT project audit, if the project is an application development or implementation project.



Copyright 2007 - Debbie Gallagher

*Debbie Gallagher is a Senior Manager, Canada IT Project Management Office at PricewaterhouseCoopers, Toronto. Debbie previously worked as a systems implementation consultant, and as IT auditor. She can be reached by email at [debbie@gallaghers.ca](mailto:debbie@gallaghers.ca).*

**MIMIX for 99.999% High Availability.  
Blair for 100% Satisfaction Guaranteed.**

The Blair Technology High Availability Services Team is the only proven Lakeview Partner in Canada that can help you achieve continuous business operations by eliminating unplanned outages and allowing you to perform scheduled system maintenance without disrupting critical business applications. As Canada's leading MIMIX and IBM Premier Business Partner of choice, Blair offers a 100% satisfaction guarantee on every high availability and disaster recovery solution they deliver.

**1 800 848 5579**  
[www.blairtechnology.com/mimix](http://www.blairtechnology.com/mimix)

**BLAIR**

© 2007 Blair Technology Solutions Inc. All rights reserved. All other company names, product names and respective company and business partner logos are registered trademarks of their owners.

