ITGC AND THE MANAGEMENT ACCOUNTANT

BY GLENN MURPHY, CMA, CPA

A strong leader in management accounting monitors data—as well as system implementations, upgrades, and improvements—through **IT General Controls**.

Information technology exists to serve the business. Management accountants must bridge the gap between IT and the business by defining the information needs, taking a leadership role, and fully participating with IT in meeting these needs. On the surface, we may appreciate the importance of Information Technology General Controls (ITGC), but are we spending the time to truly understand our organization's ITGC? As we approach the 15th anniversary of the Sarbanes-Oxley Act of 2002 (SOX), we may feel familiar with the law and its requirements. CFOs of publicly held companies routinely sign the Section 302 certification each quarter, attesting to the adequacy of their organization's internal controls over financial reporting. ITGC, sometimes referred to as General Computer Controls (GCC), are a critical aspect of these controls.

But do we know the scope of the controls and understand the internal control gaps? Are we familiar with the test plan for these IT controls? Consider that Section 302 requires the CEO and CFO, but not the CIO, to attest to reporting accuracy. When it comes to SOX and ITGC, can we really just leave IT to the IT folks?

OVERVIEW OF ITGC

ITGC are the physical, developmental, procedural, and operational control activities that monitor and protect the information systems infrastructure. This includes the hardware for data processing and storage, the telecommunications and firewalls supporting the secure flow of data, and the IT Operations personnel that maintain the hardware and software. The major components of ITGC are:

1. Information technology infrastructure:
   a. Deployment of equipment and operating systems (OS);
   b. OS updates and security patching;
   c. Establishment and monitoring of firewalls, intrusion detection systems, and other network security measures;
   d. Oversight of IT jobs occurring in file transfer protocol (FTP) sites, both between computer network applications and for other business purposes;
   e. Touchpoints of sharing with vendor/customer partner organizations—Statement on Standards for Attestation Engagements No. 16/Service Organization Controls 1 (SSAE16/SOC1) "complimentary controls" generally require secure/encrypted data standards and timely processing of information between contractual partners.
2. Infrastructure security: limitation of access to IT infrastructure to the smallest possible group and oversight of this group.
3. Systems development/change control: developing and introducing updates to technology, including critical processing applications like the enterprise resource planning (ERP) system and using a well-controlled, tested, and approved methodology that involves all key stakeholders.
4. Backup/recovery: ensuring continuity and security of critical organizational data.

5. Granting, termination, or review of user access to network directories and related data.

Application security is often included at the application/process level, but many include it with ITGC since IT typically administers application security. In either case, the business leaders bear the primary responsibility for strong application security. As management accountants, we must take a very active role in defining who can see, who can change, and who can add to the data in our systems. The IT teams understand the technology. We understand the data, as well as its purpose and value. We own the data, either directly or on behalf of the business.

BEST PRACTICES: TIER ONE

Active participation and leadership in systems implementations, upgrades, and improvements are essential activities for the management accountant. Define your information needs and stay engaged.

- Encourage your team to stay engaged with technology projects.
- Support them with effective IT training.
- Seek IMA resources to identify technology skills you need on your team.
- If you're a young professional, take advantage of your edge in technology and seek a leadership role supported by appropriate training to move your function–and your career–forward.

The 2013 COSO *Internal Control–Integrated Framework* revision raises the bar on effective internal control systems. Principle 11 in the Control Activities Component specifically requires your organization to develop effective ITGC. The Information & Communication Component includes three principles that require the development of relevant information and the means to communicate both internally and externally. Information technology is the critical platform underlying the achievement of these objectives, providing needed information to all stakeholders while protecting this information from unauthorized use.

BEST PRACTICES: TIER TWO

Once you've achieved the above objectives and established the reliability of your information systems, the next step is to leverage these systems for all critical reporting. Report from the source you've ensured is reliable rather than downloading information to unreliable, and uncontrolled, spreadsheets. Proceed to define all reports used to record information on the financials, and lock these down with change controls. Migrate as much Excel information as possible to programmed systems within the ITGC realm to reduce the risk of misstatement. Critical reports structured in business intelligence systems with effective change controls significantly reduce the risk of misstatement, not to mention the risk that employees with Excel expertise leave your organization without having provided documentation for their complicated spreadsheets.

Moving to cloud applications, hosting your data center in a secure colocation or in the cloud, or utilizing cloud infrastructure services can significantly reduce the number of ITGC your organization needs to document and test. The infrastructure controls are executed by the vendor. Security access to the infrastructure and the applications remains similar to in-house systems. Hosted applications handle all of the change controls, further reducing the ITGC requirements to the complimentary controls specified in the vendor SOC1.

Identify all of the data, its source, where it resides, who has access to it, and how it's protected. Further classify data that is proprietary or personal/private in nature. Develop a plan to protect critical data and safely discard data that is no longer needed.

Go through the same exercise with your information, asking the following questions:

- Are all stakeholders receiving the information they need, and only what they need, to perform their functions effectively?
- Is information that is no longer meeting needs routinely prepared and distributed?
- Are there better alternatives for preparing and delivering information to stakeholders?

Next, analyze the methods for delivering information. Many view the proliferation of delivering information to tablets or smartphones as a degradation of information security. Upon careful consideration, such deployments can actually enable your employees in a more secure way. Providing needed information on a tablet with no ability to download the information is more secure than e-mailing file attachments or allowing users to download information. Your data is far more secure in a business intelligence application than it is in a spreadsheet.

NEXT STEPS

A "check the box" approach to ITGC might get your organization to compliance, but not to safety and certainly not to excellence. Good governance, well-defined needs, and effective internal controls should be ends in themselves. Compliance is a by-product. Embrace your role by being a collaborative business leader with the commitment and knowledge to help your organization leverage ITGC for continued business success. **SF**

Glenn Murphy, CMA, CFM, CPA, CIA, CISA, is the cofounder of BestGRC, Inc., and founder of GRC Management Consulting, LLC. He is a member of the IMA® Technology Solutions & Practices Committee and president of IMA's Raritan Valley Chapter. You can follow him on Twitter **@GlennMurphyGRC** or e-mail him at **gmurphy@bestgrc.com**.