[redacted]

Written By: Scott Bryson

Published In: SOFE, Fall 2013

PUBLISHED ARTICLES

HELP! My ITGCs Are Weak

Assessing the Impact to Automated Controls When IT General Controls Are Weak

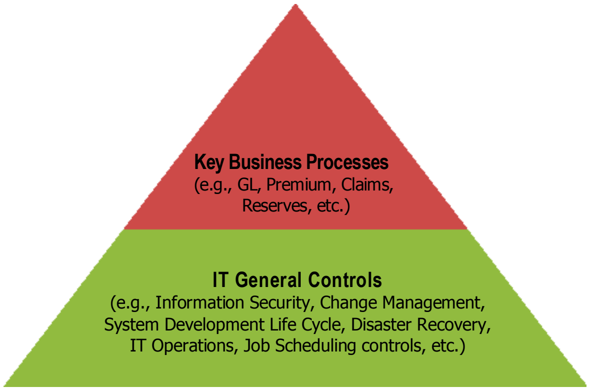
By Scott Bryson, CISA, CISSP

On a recent exam, I was asked a thought-provoking question by the Examiner-In-Charge (EIC): Even though IT General Controls (ITGCs) have been determined to be weak, may I still rely on applications controls? As an experienced IT examiner, I had a response in mind but thought it would be a good exercise to compare my answer to industry recommended practices.

Let's start by performing a quick review of ITGCs and application controls.

By definition, ITGCs are controls that apply to all systems components, processes, and data within an organization or information technology (IT) environment. ITGCs are implemented to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations. ITGCs fall into the following categories: Computer Operations, Security, Systems Development, Change Management, Backups and Disaster Recovery. ITGCs provide the foundation upon which business processes rely. Controls in these categories have been well documented and tested by IT examiners for many years. The diagram shows that ITGCs are the foundation for a reliable Information Systems processing environment. Strong ITGCs allow the IT examiner to conclude that the IT environment is effective and can be relied upon for the purposes of the financial exam.

Over the past five to ten years, greater attention has been paid to application controls by financial and IT examiners. Application Controls have become an increasingly important topic of discussion between the financial and IT examiners. Application controls are those controls that pertain to the scope of individual business processes or application systems, including: data edits, separation of business functions, balancing of processing totals, transaction logging and error reporting. [1] Application controls are an important part of today's risk-focused examination (RFE) process, and, if tested properly, favorable results can reduce the level of substantive testing required to be performed by the financial exam team.


Key Business Processes
(e.g., GL, Premium, Claims, Reserves, etc.)
IT General Controls
(e.g., Information Security, Change Management, System Development Life Cycle, Disaster Recovery, IT Operations, Job Scheduling controls, etc.)

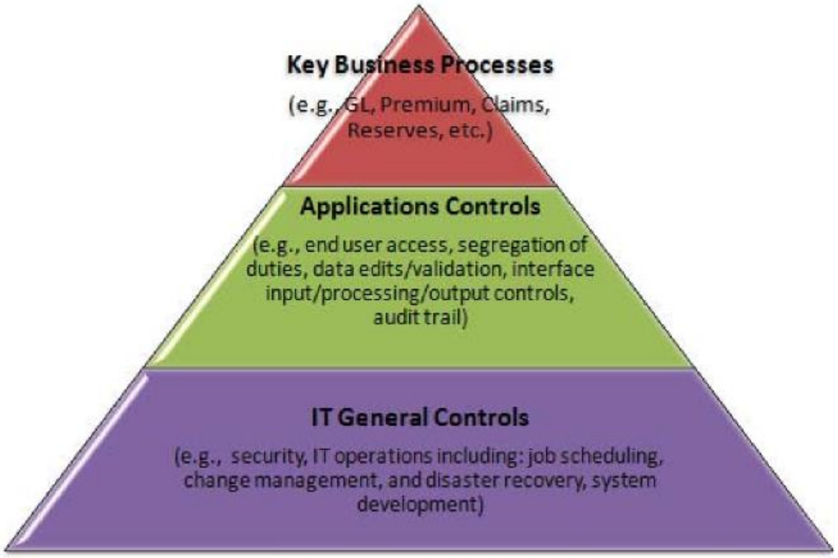
HELP! My ITGCs Are Weak

Assessing the Impact to Automated Controls When IT General Controls Are Weak

(continued)

COBIT defines application controls as "a subset of internal controls that relate to an application system and the information managed by that application. They are designed to ensure timely, accurate and reliable information to enable informed decision making... They consist of the manual and automated activities that ensure that information conforms to certain criteria... including: effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability."2

Application controls sit between ITGCs and a company's business processes (See diagram). Application controls include: completeness (input, processing and output), accuracy (claim cannot be paid if incurred prior to member effective date), validity (valid ZIP code), authorization (authority limits), and segregation of duty controls. An example of an application automated control is a ZIP code edit. For example, consider that a health insurance plan often bases the reasonable and customary reimbursement rate for an outpatient procedure on the provider's ZIP code. When a claim is entered into the insurance company's claim system, either automatically or manually, the application logic validates the provider's ZIP code on the claim with the ZIP code in the provider database and then determines the reimbursement rate for the procedure based on the provider's ZIP code.


Key Business Processes
(e.g., GL, Premium, Claims, Reserves, etc.)
Applications Controls
(e.g., end user access, segregation of duties, data edits/validation, interface input/processing/output controls, audit trail)
IT General Controls
(e.g., security, IT operations including: job scheduling, change management, and disaster recovery, system development)

In addition to ensuring the data is accurate, application controls also help ensure that the data is complete. For example, consider the following scenario:

Healthcare claims received electronically are received from one or more healthcare clearinghouses. The electronic claims may be systematically checked to validate that they are in a HIPAA compliant transaction format and may be assigned a claim number. Any claim that does not pass the HIPAA

HELP! My ITGCs Are Weak

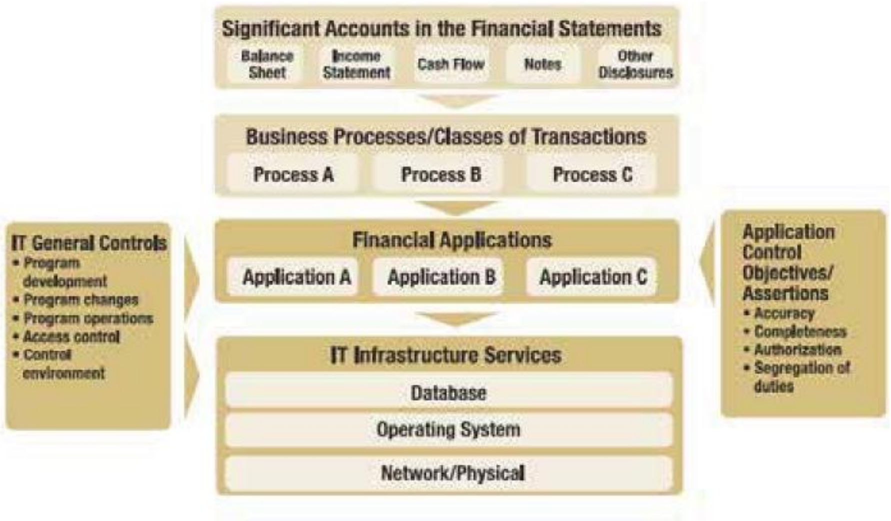
Assessing the Impact to Automated Controls When IT General Controls Are Weak

(continued)

validation is returned to the submitting provider via the clearinghouse for correction. All claims that pass the HIPAA validation are loaded into the claim system. The claim system automatically acknowledges the receipt of the claim to the company's EDI Operations area. On a daily basis, EDI Operations reviews the status of all claims received from the clearinghouse, and it is loaded into the claim system or returned to the submitter. Any out of balance conditions are resolved.

In relation to the above scenario, a control the company may have in place to ensure that all electronic claims are loaded into the claim system may be: "All electronic claims loaded into the claim system are reconciled back to the EDI clearinghouse." This example illustrates an automated control that also has a manual reconciliation element (i.e., the system automatically generates the report and the report is reviewed by EDI Operations).

Next, it is important to understand the relationship between ITGCs and application controls. Below is a diagram, published initially for Sarbanes-Oxley purposes but does a good job showing how each of the types of controls supports processing:



As depicted in the above diagram, ITGCs apply to both the application and infrastructure level. ITGCs are required to support the effectiveness of application controls. If critical ITGCs (e.g., primarily logical security and change management controls) are found to be ineffective, application controls should not be relied upon. Here is an analogy that we often present when explaining the relationship between these two levels of controls. It is a bit like thinking about building a house—you cannot build a house without first pouring a solid foundation. If there are cracks in the cement, issues likely will be present later on when the rest of the house is constructed.

HELP! My ITGCs Are Weak Assessing the Impact to Automated Controls When IT General Controls Are Weak

(continued)

I performed some research to validate my perspective against those positions of industry experts. Below are some sample excerpts of what I found.

SOURCE	LANGUAGE
IT Control Objectives for Sarbanes-Oxley, 2nd Edition	The relationship between application controls and IT general controls is such that IT general controls are needed to support the reliability of application controls. For example, ensuring database security is often considered a requirement for reliable financial reporting. Without security at the database level, companies would be exposed to unauthorized changes to financial data. The PCAOB describes IT general controls as having a "pervasive" effect over all internal controls. That is, if a relevant IT general control fails (e.g., a control restricting access to programs and data), it has a pervasive impact on all systems that rely on it, including financial applications. As a result, without being assured that only authorized users have access to financial applications, companies are unable to conclude that only authorized users initiated and approved transactions.)
COBIT and Application Controls – A Management Guide: ISACA 2009	Applications and application controls depend on a reliable IT processing environment for their continued effectiveness. IT general controls are those controls within the IT processing environment that provide for this ongoing reliability (e.g., information security and change management controls, IT operations and job scheduling controls). As such, failures or breakdowns in IT general controls can have a significant impact on the effectiveness of the application controls. Therefore, it is important that the effectiveness of IT general controls be understood throughout the application control design, implementation, operation and maintenance activities. A strong system of IT general controls can enable more reliance on automated application controls, whereas a less reliable system of IT general controls may suggest that greater emphasis should be placed on manual controls. Issues or failures in IT general controls may create a ripple effect, impairing the reliability of automated application controls and potentially impacting the integrity of the business processes and data.

HELP! My ITGCs Are Weak

Assessing the Impact to Automated Controls When IT General Controls Are Weak

(continued)

	LANGUAGE
GTAG Auditing Application Controls, July 2007	In addition, it is important for Chief Audit Executives to note the degree to which management can rely on application controls for risk management. This
	reliance depends directly on the design and operating
	effectiveness of the ITGCs. In other words, if these
	controls are not implemented or operating effectively,
	the organization may not be able to rely on its
	application controls to manage risk. For example, if the
	ITGCs that monitor program changes are not effective, then unauthorized, unapproved, and untested program changes can be introduced to the production environment, thereby compromising the overall integrity of the application controls.

It seems like the industry experts agree — application controls are reliant on ITGCs.

In summary, ITGCs and application controls are both critical to an entity's control environment. ITGCs are the pervasive controls that support all company systems. Application controls, which are implemented specific to each application, rely on a strong set of ITGCs for continuous and reliable processing. If ITGCs are tested and determined to be weak and/or ineffective, application controls should not be relied upon.

ENDNOTES

1 – Bellino, Christine; Hunt, Steve; "Auditing Application Controls," Global Technology Audit Guide (GTAG) 8, IIA, July 2007

2 – ISACA, "COBIT and Application Controls – A Management Guide," ISACA, 2009

3 – ISACA, "IT Control Objectives for Sarbanes-Oxley, 2nd Edition," ISACA, November 2006

About the Author

Scott Bryson, CISA, CISSP, is a manager and IT specialist with Risk and Regulatory Consulting, LLC, where he performs risk based IT security and controls assessments and compliance consulting services for state regulators at a broad range of insurance entities. He specializes in IT Security controls assessment and compliance, with an emphasis on federal and state IT regulatory compliance (SOX, HIPAA-HITECH), IT controls design, SAS70/SSAE 16 assessments, disaster recovery, IT outsourcing and off-shoring, IT governance, business continuity, change management, information security, computer operations and e-business. Scott can be contacted at scott.bryson@riskreg.com or 860-543-0038.

.