Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

Scoping ITGC'S for SOX 404 Audits

by

PERHR, Trish

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Date: May 2008

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Ron Ruhl, Director and Associate Professor, MISSM

Scoping ITGC'S for SOX 404 Audits

by

PERHR, Trish

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Ron Ruhl, Director and Associate Professor, MISSM

Reviews Committee:

Andy Igonor, Assistant Professor, MISSM
Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

Date: May 2008

The author acknowledges the significant contributions to the work by Academic Advisors and Review Committee Members and gives the right to Concordia Univeristy College to reproduce the work for the Concordia Library, Concordia Websites and Concordia MISSM classes.

Scoping ITGC's for SOx 404 Audits.

Combining frameworks and/or methodologies to achieve efficiencies and effectiveness.

Trish Perhar, BSc, After Degree Diploma ISSM

Concordia University College of Alberta

May 2008

Table of Contents

Abstract

Scoping IT general controls (ITGC's) for the purpose of complying with legislation such as Section 404 of the Sarbanes-Oxley Act has been no simple feat. Both management and auditors alike have faced challenges in terms of scoping the work that is to be performed around ITGC's. The Public Company Accounting Oversight Board (PCAOB) and the U.S. Securities and Exchange Commission (SEC) advocate the use of a top-down risk based approach to define the scope of work for Section 404 compliance. However, the use of this approach is not yet fully understood and is not being completely followed. Methodologies are available and have been created to assist with scoping and assessing ITGC's, as described in this paper, however extensive resources are still being utilized to comply with Section 404. This paper reviews current industry practices, by analyzing methods and approaches towards ITGC scoping, for a sample of three companies in differing industries. This review is then followed by an analysis of a newer methodology, the GAIT methodology, and how this new methodology can create efficiencies in the scoping of ITGC work, relative to current practices.

1.0 Introduction to SOx 404 Compliance

1.1 Background

The Sarbanes Oxley Act of 2002, also known as SOx, is a U.S. federal law which was enacted in response to a number of major accounting scandals. Initially, the SOx act was conceived in a congressional committee in December 2001 after the Enron scandal. While this bill was being considered in the U.S. Senate, the WorldCom accounting scandal came to light. As a result of this additional corporate fraud, the SOx bill was then expanded to include Section 404: Assessment of Internal Controls (Section 404) which was enacted on July 30, 2002.

Section 404 is the most contentious aspect of SOx as it requires management and the external auditor to report on the adequacy of a company's internal control over financial reporting (ICFR). Management is expected to administer alignment between IT practices and business practices and between technology management and financial management. Due to a large reliance on information systems for financial reporting, IT has become a large and crucial piece of the ICFR puzzle for Section 404 compliance. ITGC's provide a level of reasonable assurance that key application functions are operating consistently. ITGC's exist as preventative and detective type controls, helping to protect data and programs from unauthorized change. They assist in the determination of whether material errors would have impacts to financial statements.

In order to achieve ICFR, frameworks, methodologies and standards were made available to assist with identifying, defining, assessing and testing internal controls relevant to financial reporting.

1.2 Standards/Frameworks/Methodologies

1.2.1 PCAOB's AS2 and AS5

SOx mandated the creation of a new entity to create and oversee public company auditing standards and practices. The Public Company Accounting Oversight Board (PCAOB) was then created. The PCAOB's mission is to oversee the auditors of public companies and protect the interests of investors through the setting of standards. These standards are subject to the approval of the U.S. Securities and Exchange Commission (SEC) which oversees and regulates the securities industry in the U.S. and enforces securities laws.

The PCAOB published an auditing standard that outlined the procedures auditors should use when auditing management's internal controls over financial reporting. This document, Auditing Standard No. 2 (AS2), described to companies what auditors would be looking for when they were performing their assessments. AS2 was designed to encourage auditors to use a top-down risk based approach as it would prevent the company from spending unnecessary time and effort documenting or testing a process or control that would be unlikely in detecting a material misstatement. The top-down risk based approach enabled auditors to focus early on in the process on items that may have an effect on the auditor's final decisions about scoping and testing strategy. As such, IT executives were required to evaluate the impact of AS2 on their IT controls program as AS2 did not explicitly detail which IT controls were to be included in the assessment.

It was noted, however, through a second year implementation study conducted by the PCAOB[1] that companies using the AS2 were doing far more work around ITGC and control defining and testing than was necessary. Companies filing for ICFR were not

effectively scoping their IT work[2]. Appropriate risks were not being addressed and in some cases every possible control was being tested. Many companies did not have a complete understanding of the top-down risk based approach and this resulted in a lack of the quality of controls and testing that was conducted for the ICFR audit.

What is the top-down risk based approach?

A top-down risk based approach focuses on those areas of the financial statements that present significant risk that the financial statements could be materially misstated if the controls are not functioning effectively. A top-down risk based approach begins with an understanding of the risks inherent to the financial statements and by determining the significant accounts, account components, relevant assertions, and classes of transactions that contribute to those risks. This approach also considers how company-level controls address inherent risk of misstatement in significant accounts, account components, relevant assertions, and classes of transactions.

Updates were made to PCAOB's AS2 and it was superseded by AS5 in July 2007. The new standard, AS5, required auditors to tie compliance directly to their financial reporting through a top-down risk based approach. A relationship must exist between the risk of a material weakness and the amount of attention given by the auditor to that area. A higher level of detail was provided within AS5 with regards as to when to use the top-down risk based approach[3]. It addresses multi-location testing and instructs auditors to use a top-down approach when scoping work at various company locations instead of the original three categories of location testing provided in AS2.

This top-down risk based approach is one way in which effectiveness as well as efficiencies can be created during an audit. This approach focuses the compliance process

on those business processes that are significant to financial reporting. There is assurance that appropriate risks are being addressed, as critical business processes are being defined.

1.2.2 COSO

Furthermore, SOx guidance required the usage of an internal control framework. The SOx legislation references the Committee of Sponsoring Organizations of the Treadway Commission framework (COSO). COSO provides an integrated framework to assist businesses in assessing and enhancing their internal control systems and by aligning their IT governance practices with SOx. COSO's Internal Control Integrated Framework states that internal control is a process that is established by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of stated objectives[4]. However, while COSO provided a useful overall framework for internal controls, it did not provide detailed guidance on IT-specific controls. Since IT management did not have detailed guidance with regards to IT-specific controls, they had to look elsewhere for an IT-specific framework.

1.2.3 ISACA's CobIT

Prior to the inception of SOx, the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) had developed a set of best practices framework for IT management, namely, Control Objectives for Information and related Technology (CobIT). CobIT provides the necessary guidance that was missing from COSO, related to IT-specific controls. CobIT details a set of generally accepted

measures, indicators, processes, and best practices, to assist in maximizing benefits through the use of information technology and developing appropriate IT governance.

The first version of CobIT was released in 1994 (CobIT 1.0) and since then there have been three major releases of the CobIT framework with the most recent being released in May 2007. In the first two years of filing for ICFR, full versions of the CobIT 3.0 framework were most widely used (released in 2000). Modifications were made from version 3.0 to 4.0 in December 2005. This modification included an update to increasing IT management's focus as well as increasing maturity of IT best practices and standards.

It was noted that, for the most part, CobIT follows a siloed approach to classifying ITGC's through which similar controls are kept separate as they are relevant to different departments, applications, or business process owners. ITGC's are classified in columns making it difficult to address risks in this method of organization. Many companies were using more controls than were necessary for the ICFR process, therefore creating inefficiencies in their testing procedures. Not all risks were being addressed through the use of CobIT since the area that CobiT covers is fairly large.

1.2.4 ITGI's "CobIT - lite"

A modified version of CobIT, made more specific to those companies filing for ICFR, was released initially in 2004 by the ITGI, namely, the IT Control Objectives for Sarbanes-Oxley[5] (CobIT-lite). The second version of CobIT-lite was released in September 2006. The purpose of this document is to "share lessons learned from companies and provide additional guidance on how to improve the efficiency and effectiveness of compliance using a risk-based approach."[6]

CobIT-lite has not received endorsement from the PCAOB nor the SEC. It is also noted in this document that "… each organization should consider the appropriate IT control objectives necessary for its own circumstances. Organizations may choose not to include all the control objectives discussed in CobIT-lite, and similarly they may choose to include others not discussed in this document."[7] The CobIT-lite document was created prior to the PCAOB's adoption of the new AS5 standard, and does not take into account guidelines provided by the PCAOB with regards to the top-down risk based approach. It does explain a detailed top-down risk based approach and it incorporates risk assessments as a part of the scoping process. CobIT-lite focuses on what is required for financial reporting, however, its objectives and considerations in the document may exceed what is necessary to comply with Section 404.

Compared to the first edition published in 2004, "certain controls in Appendix C, IT General Controls, have been identified as most relevant controls". The disclaimer of this document states that "the contributors make no representation or warranties and provide no assurances that an organizations use of this document will result in disclosure controls, procedures, internal controls and procedures for financial reporting that are compliant with the internal control reporting requirements of the Sarbanes-Oxley Act"[8].

Since this document has not been endorsed by a governing body, there is a large risk with using it and consequently companies have to use their best judgment when using it.

1.2.5 IIA's GAIT Methodology

Developed by the Institute of Internal Auditors (IIA) and a core team of 7 individuals, the Guide to the Assessment of IT General Controls Scope Based on Risk

(GAIT) was released in January 2007[9]. The IIA and its team began working on this method, which comprises of a set of Principles and a Methodology to facilitate the cost-effective scoping of ITGC assessments and audits, by adopting the top-down risk based approach. Based on a response by the co-chair of the GAIT Project Advisory Board, Thomas Ellis, "…GAIT helps improve the cost effectiveness of IT general controls auditing by including within audit scope all and only those elements or layers of IT infrastructure and IT general control processes that are relevant to financial reporting risks".[10]

The principles of GAIT address a concern identified by the PCAOB with regards to public companies compliance with Section 404 - the scope of ITGC's. The very first Principle of GAIT states that GAIT continues the top-down risk based approach in AS5 using those results to help users identify potential failures in IT general control processes that could lead to errors on financial statements. Another Principle of GAIT is that the scope of Section 404 work only needs to address risks in ITGC processes that would represent a likely risk of material error in financial statements. The Methodology of GAIT consists of an extended discussion of the Principles, process documentation, as well as customization of GAIT based on a company's individual needs. This methodology has been implemented at organizations that have been part of the development of GAIT, such as Microsoft Corp.

1.2.6 Comments

While focus has been provided on what is required for financial reporting, the control objectives and considerations mentioned in CobIT-lite may exceed what is necessary for companies seeking to comply with the requirements of SOx. The suggested

internal control framework, COSO, to be used for compliance with SOx, addresses the topic of IT controls, but does not mandate requirements for such control objectives and related control activities. Similarly, PCAOB's AS2 states the importance of IT controls, but does not specify which controls in particular must be included. Such decisions remain the discretion of each company. Accordingly, companies should assess the nature and extent of IT controls necessary to support their internal control program on a case-by-case basis. Details have been provided in AS5 as to the required top-down risk based approach, however it is still dependant on the company to interpret the guidance.

GAIT presents a granular approach in determining specific ITGC objectives and key controls by assessing risks at different levels of the IT infrastructure. It also considers risks within each ITGC process. GAIT enables management to identify key ITGC's as a part of the continuation of a top-down risk based approach. This methodology is relatively new, as compared to the previous methodologies discussed and many companies have not yet considered its use.

Section 404 has been the most costly aspect of the overall SOx legislation as it has required a tremendous amount of time and effort to document and test critical financial manual and automated controls. Most, if not all public companies that have filed for compliance to SOx since 2002 have incurred excessively large compliance costs. These high costs include work involving ITGC's. Based on a survey completed by the Institute of Internal Auditors in January 2007, 30% of the respondents stated that 21-30% of their overall SOx costs relate to ITGC work[11]. That is a substantial portion of IT costs, relative to overall costs associated with Section 404 compliance.

If the scope of ITGC's is not addressed appropriately, there is a large chance that not all material risks will be addressed, decreasing the effectiveness of the audit and increasing the overall risk of material misstatements on financial reporting. In addition, if the scope of ITGC's is not addressed appropriately, there will be a decrease in the efficiency of the audit, costs will increase, the number of resources will rise, and the amount of unnecessary work for Section 404 compliance will also increase.

Many companies have encountered some of these issues, due to the fact that their ITGC scope was not addressed appropriately.

2.0 Sample Industry Practices

We obtained ITGC scoping documents and methodologies from a sample of 3 companies[12], from differing industries.

2.1 Company A

Company A is from the oil and gas industry. Like many oil and gas companies, this is a large company, with many entities. Company A's IT environment is fairly large and complex. Applications and systems used by this company are in house developed programs. They do not use any Enterprise resource planning systems (ERP's). Company A is in its third year of SOx compliance. They began their scoping process for ITGC's using CobIT 3.0 and then moved on to the CobIT-lite version when it was released. In their first year of compliance they had approximately 40 applications in scope. At year three, this company has based all their scoping, identifying, assessing and testing on the CobIT-lite framework and have approximately 15 in-scope applications.

Of the in-scope processes as determined by CobIT-lite, Company A determined which of these processes applied to their company, for example, since they did not

purchase all the software off the shelf and were producing it themselves, they needed to include controls around program, software, and development. Once these controls were selected, an IT risk assessment (as per CobIT-lite[13]) was performed, identifying each of the processes and its controls as high, medium or low risk. Company A defined these risks as follows: 'High' - for those controls with a significant impact on financial statements, 'Medium'- less significant impact on financial statements, and 'Low' - very little to no impact on financial statements.

The reduction in the number of in-scope applications does not reduce the risk of not identifying all potential risks of material misstatements, as applications that were once deemed critical, are now not financially significant. In the first year of compliance Company A yielded a large number of in-scope applications as a result of using the CobIT 3.0 framework in which all financial systems were critical, and not only those which can be the cause of a material misstatement on financial reporting, for ICFR purposes.

Company A is placing more emphasis on entity level controls in which a direct relationship with lower-level controls can result in a decreased testing effort, resulting in lower costs associated with compliance. They would like to use benchmarking[14] on their IT controls, however since they have a large number of in-scope applications still, they have not yet been able to reach this.

2.2 Company B

Company B is an engineering/consulting firm. This firm is in its third year of compliance as well. They initially used the CobIT 3.0 framework with regards to scoping, defining, and assessing ITGC's, however switched over to CobIT-lite version 2 in 2007.

The IT environment for this company is very complex as acquisitions and mergers are made on a regular basis. They have established a baseline approach to work for this year - since ITGC's have been effective in the past year, they will be relying on tests performed from last year, provided the review of ITGC's concludes that they have been designed and are operating appropriately. Though the exact number of controls is not available, this company has decreased their number of key controls since their first year of compliance. The main reason for a decrease in key controls was a re-evaluation of risk - eliminating the need for testing low as well as some medium risk controls.

2.3 Company C

Company C is a company in the insurance industry. This is a very large company and has several numbers of entities within. They are currently working on their first year of compliance for Section 52-109, the Canadian version of SOx. They have over 100 critical ITGC's to review and test. Their list of significant financial applications is quite large and this list consists of mainly in house systems. Many of the systems feed off of each other, thereby making this IT environment a largely complex one. In addition, since Company C acquires smaller companies, the IT systems of the smaller entities are also included on the significant financial applications listing and each of them have their own complex IT environments. This company has in no way tried to consolidate financial systems. There are several payroll systems, several invoicing systems, several accounts receivables systems, etc.

Company C has applied the full CobIT 4.0 framework, not the CobIT-lite framework, which explains why there are such a large number of controls for testing. Company C does not seem to have the most effective use of time and resources,

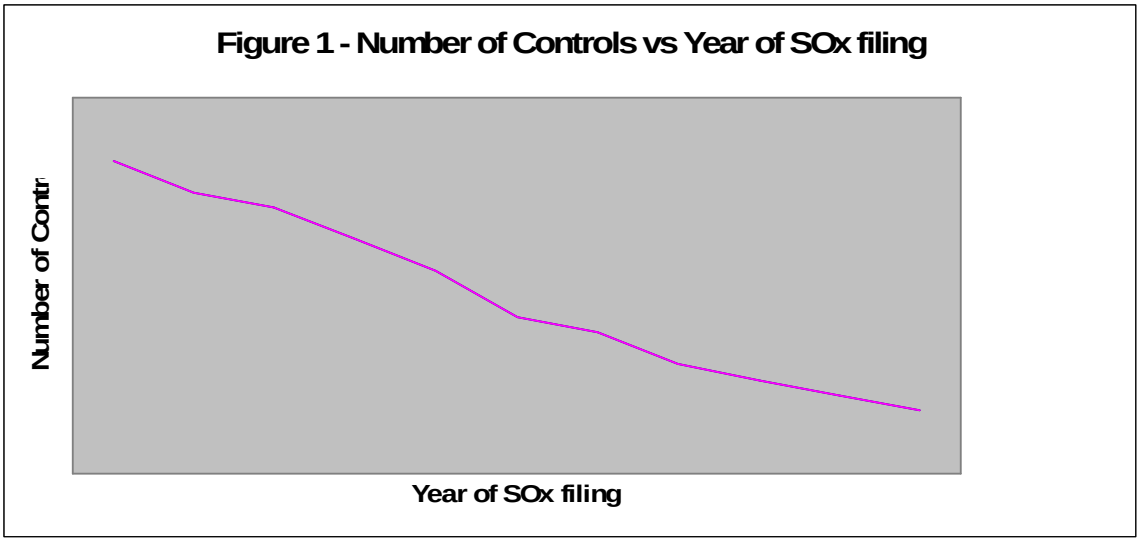
especially if the company is using the full CobIT 4.0 framework and not the 'lite' version. CobIT 4.0 is a large framework and covers pretty much everything in IT. Company C are also not following the prescribed top-down risk based approach in which case controls identified may be assessed and tested that are not critical. This results in a higher than needed cost and a consumption of resources.

2.4 Analysis of Sample Companies' Methodology Review

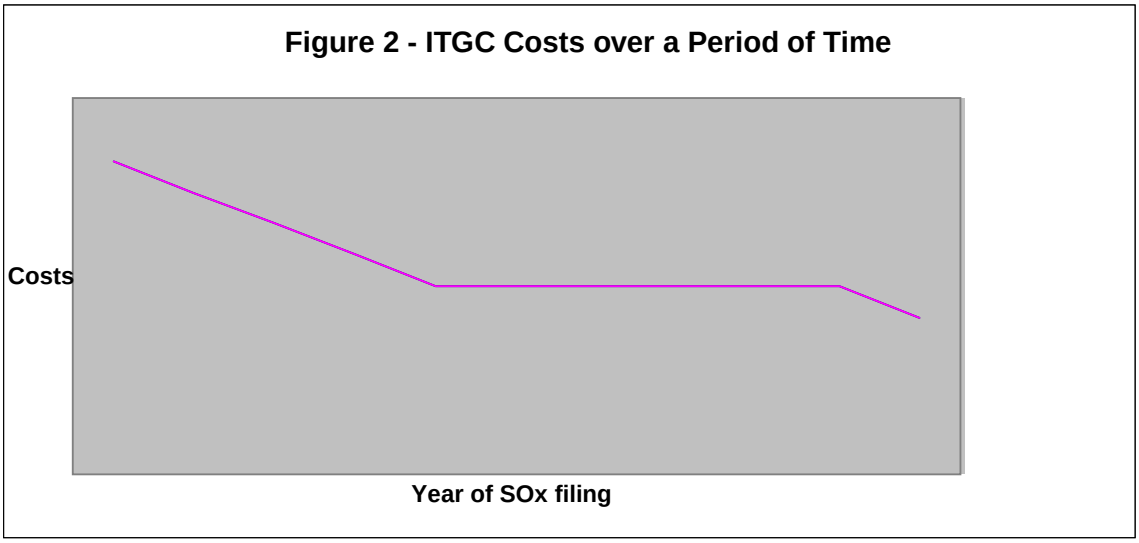
2.4.1 Companies A and B

For early SOx filers such as company A and B, methodologies and understanding of Section 404 was not as developed in comparison to recent methodologies and updates to existing standards. Company A and B, along with many advanced filers, had to complete work around ITGC's, CobIT was recommended and it was the most widely available framework. Due to the vast area of IT that is covered by CobIT, both these companies provided more than what was necessary for compliance auditing. They did not know what the minimum requirements for SOx were and so costs for these advance filers ended up being extensive. They began using CobIT-lite upon it's release as CobIT-lite detailed lessons learned from initial filings as well as it described, to greater detail than what was provided before, on how to use the CobIT framework for the purposes of evaluating IT controls in support of SOx compliance.

From the analysis of both Company A and B, as the number of years of Section 404 compliance increase, the number of controls has been decreasing (Figure 1).



As a result of a decrease in the number of controls over time, ITGC costs also decrease (Figure 2). There are fewer controls to test and assess.



Initial costs of scoping ITGC's were high for both Company A and B as well as for advance filers. There were a large number of controls and there was a large learning curve for filers as well as auditors. However, over a period of 3 years, both Company A and Company B had a large reduction in the number of key controls that required testing.

This was a result of optimizing the use of a methodology, specifically, CobIT and the CobIT-lite methodologies. As time goes on, the numbers of controls are expected to decrease, assuming that business processes are held constant, i.e. systems are not changed and/or replaced. However the goal of efficient compliance is not to decrease the number of ITGC's; this may result in an ineffective audit. The goal is to ensure that all risks to financial reporting are addressed. Initial identification of controls may not relate or have any risk to financial reporting. Once a control is scoped to a detailed level it can be removed from next year's Section 404 compliance audit scope.

What would have benefited companies A and B three years ago when they were first filing for compliance, was a methodology that went into detail on how to use the top down risk based approach to scope ITGC's from the get go. This would have saved first year costs as will be discussed in section 3.0 on GAIT.

2.4.2 Company C

Similarly, Company C is now undergoing much of the frustrations and headaches that Company A and B had several years ago. However, the difference in this company's case is that newer methodologies are available, such as GAIT and modifications to AS5 have been made with regards to the top-down risk based approach. This provides quite a bit more guidance than what was available for Companies A and B when they were filing. Company C's costs are going to be considerably high, considering they are using the CobIT framework.

3.0 Efficiencies in Scoping ITGC's

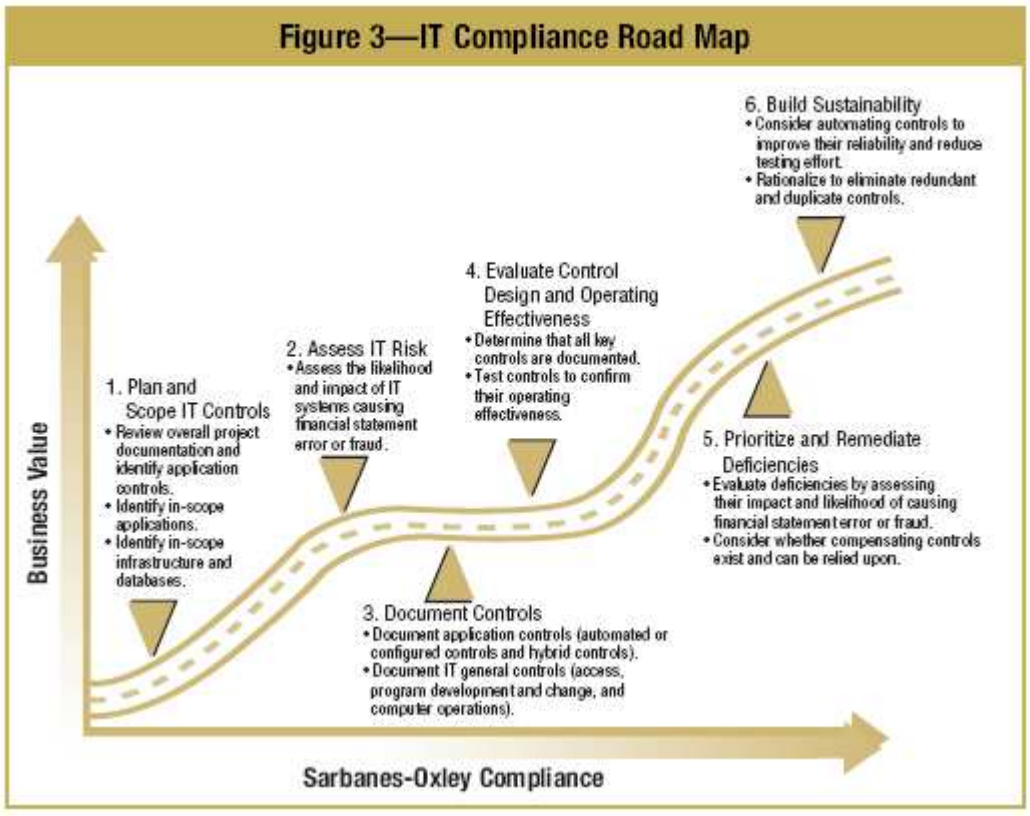
As has been discussed in this paper thus far, there has been a lot of time and money spent on work around ITGC's. It was noted that initial costs of compliance were large, and this was due to a lack of understanding and guidance available at that time. Advance filers have recently started using CobIT-lite in their ITGC work, clarifying some misunderstandings from filing early on. Many of these companies have optimized their use of the CobIT-lite framework and have reached a level with audit reporting that they are comfortable with. Relative to the sample companies discussed earlier, these would include Companies A and B. Over a period of three years, in both of these companies, they have reached their comfort zone and would be less than willing to adopt a new framework.

Efficiencies in the scoping of ITGC's can be created, however it is more difficult to apply a new scoping framework appropriately (as will be discussed further in this paper) for those companies who have already made an existing framework applicable to their IT environment, business processes and overall organization. The GAIT methodology, released in early 2007, has the potential to create efficiencies with regards to the ITGC scoping process. This methodology however is targeted more towards companies filing for ICFR for the first time. Since CobIT-lite was the dominant framework used in the sample companies' analysis above, a comparison between its use and GAIT will now be discussed.

3.1 CobIT-lite and GAIT

A large difference between GAIT and CobIT-lite is that GAIT continues the top-down risk based approach beyond the financial statement level, whereas CobIT-lite does not. GAIT presents a granular approach in determining specific ITGC objectives and key controls by assessing risks at different levels of the IT infrastructure. It also considers risks within each ITGC process. GAIT enables management to identify key ITGC's as a part of the continuation of the top-down risk based approach.

CobIT-lite illustrates an IT Compliance Road map[15], as shown below:

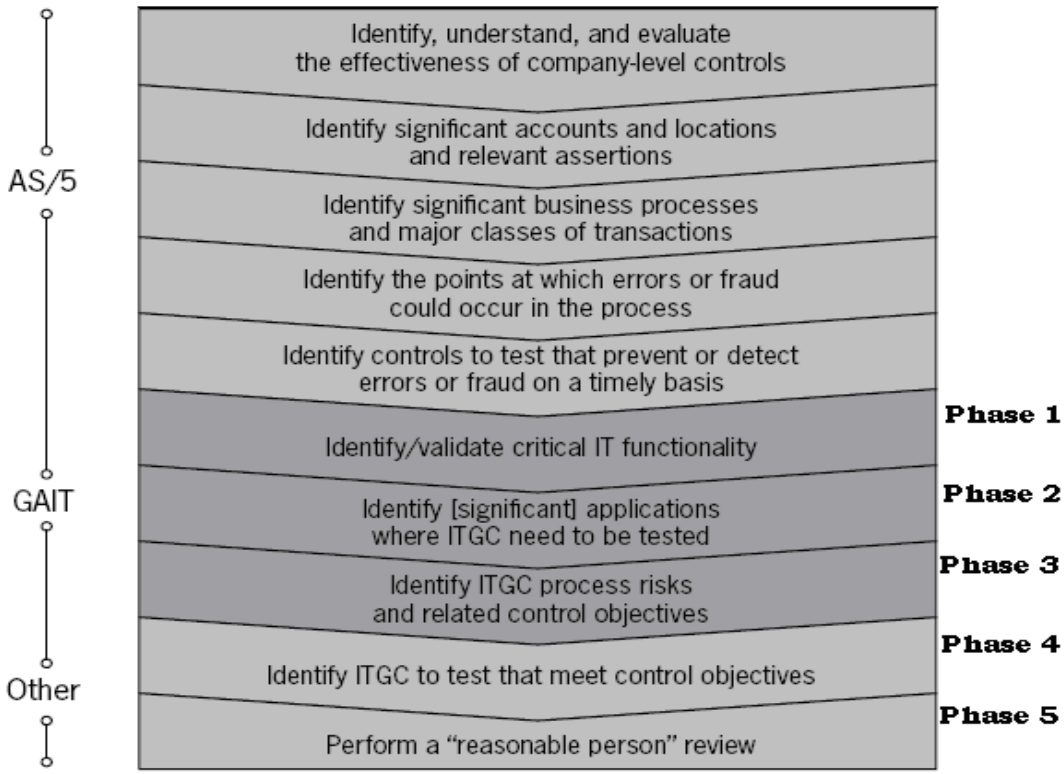


This roadmap "provides direction for IT professionals on meeting the challenges of the Sarbanes-Oxley Act."[16] Here is a summary of what the IT Compliance Road Map illustrates: Planning and scoping IT controls and Assessing IT Risk are the initial steps in IT compliance. Both have little business value, but at the same time, both are huge steps

towards Section 404 compliance. It is at these two initial steps that project documentation is reviewed and application controls are identified from the in-scope applications. IT risk is assessed. The next step details the documentation of controls. This is shown to have very little business value, and is conducted later on in the Section 404 compliance process. Next (step 4) is the evaluation of control design and operating effectiveness. It is at this step that documentation of key controls and testing for operating effectiveness occurs. Prioritizing, remediation and building sustainability are the final steps in the IT Compliance Map. Deficiencies are evaluated, compensating controls are identified, and consideration for the removal of controls is made.

The following table can be found within the GAIT methodology and it details the flow of GAIT's top-down risk based approach to the scoping of ITGC's beginning with AS5's top-down risk based approach, and continuing with this same approach throughout[17].

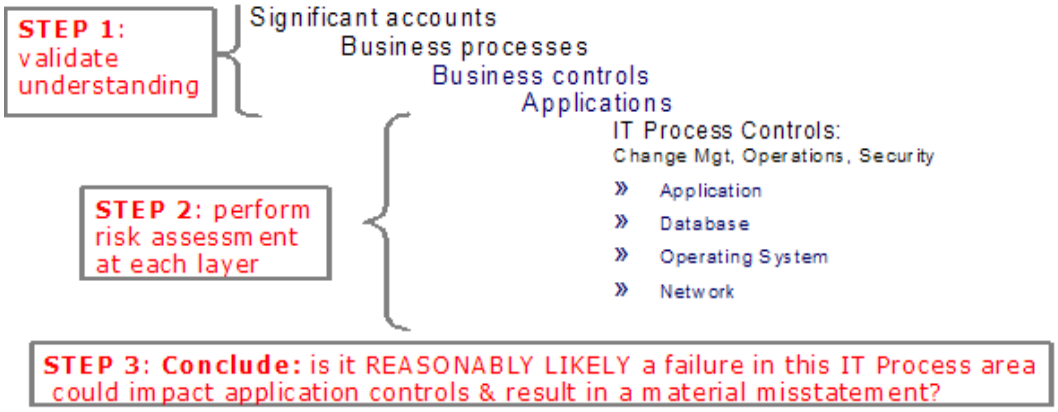
Figure 4 *Top-down process, including GAIT*



This methodology contains five phases as noted in the table above. In the identification and validation of critical IT functionality stage (phase 1), as a continuation of the top-down process, GAIT confirms the identified key manual and automated controls. This ensures that all critical IT functionality has been identified. This listing of key manual and automated controls is then used in the next step (phase 2) which is the *identification of key applications where ITGC's need to be tested.* Since critical IT functionality has now been confirmed, financially significant applications can be identified. As per GAIT, "financially significant applications are those where there is a potential ITGC process risk because they contain critical IT functionality or data." [18] This eliminates the need of addressing applications that are involved in the processing of either financial transactions which are not critical to IT functionality or data which is subject to illicit changes, which would not be in scope for Section 404. Continuation into the phase

3 can only be accomplished with financially significant applications. The goal of this phase is to try to link each key ITGC to the control objectives identified. Questions addressed in this phase include: "What is the likelihood of a process failure occurring and what is the potential impact? What is the likelihood of IT process failing in such a way that it would cause critical IT functionality to fail?"[19] When implementing GAIT, it is critical to remember that GAIT only helps to determine if a control is within scope for SOx compliance. It is not used to place or remove anything from the compliance scope. A summary of GAIT[20] is illustrated below:

Figure 5 Summary of GAIT

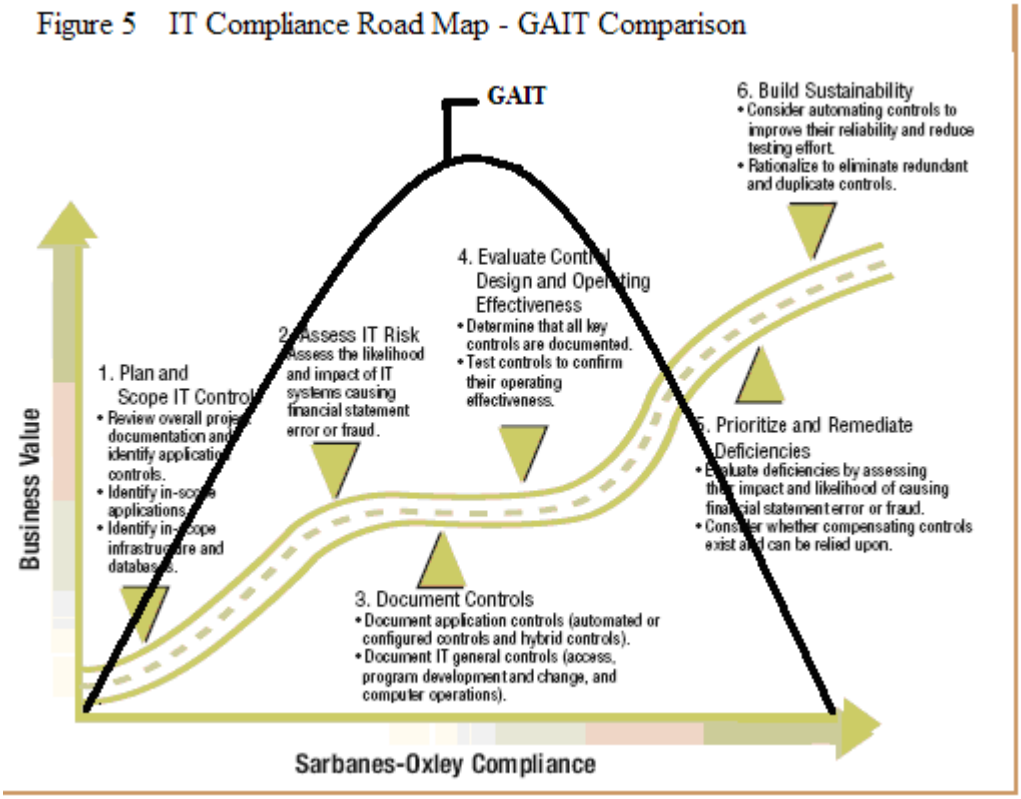


As you progress downwards to Step 3, the number of controls will decrease from initial ones identified in Step 1.

Relative to the CobIT-lite IT Compliance Road Map in figure 3 above, GAIT's approach is very streamlined. All phases of GAIT potentially increase the business value as each phase progresses, and it is all done in a timely manner. This creates efficiency as compared to CobIT-lite as GAIT eases its way into the IT Compliance Road Map directly into Step 4, evaluating control design and operating effectiveness.

As compared to the IT Compliance Road Map, GAIT's approach would have a road map similar to the following figure:

Figure 5 IT Compliance Road Map - GAIT Comparison



Efficiencies are created as there is a linear relationship between the business value and the time for compliance. GAIT covers the majority of the planning of IT controls, assessing IT risk, documenting controls in a very detailed manner. Costs are at their peaks when it comes time to documenting and testing controls. Once those have been completed, costs to the business decrease.

For the remaining two phases of GAIT, phases 4 and 5, GAIT recommends using another framework in the determination of specific key controls. CobIT is mentioned in the GAIT document as a framework that can help "significantly". In these steps, IT process risks and related control objectives are identified. Phase 4 in GAIT is to identify the ITGC's that meet each of the IT control objectives determined in the phases previous

to this. For this, the use of CobIT-lite would accomplish the task. CobIT-lite details control guidance for each section within each business process. This includes control guidance for manage changes, enable operations, and manage third-party services, to mention a few.

For Steps 5 of figure 3, the IIA has established a practice guide, titled “GAIT for IT General Control Deficiency Assessment. In this guide, a discussion of the approach to the assessment of ITGC deficiencies is made. This helps with the assessment of whether the deficiency is a material weakness or a significant deficiency.

GAIT’s intention is not to reduce control numbers; however it has been found that companies who have been utilizing GAIT, have noticed a decrease in numbers of controls. This is a result of eliminating redundant controls and those controls which do not represent a likely risk to financial reporting. By using GAIT along with CobIT, a more efficient process is conducted to scope ITGC’s through GAIT’s use of the top-down risk based approach. Control objectives are based on risk to the financial statements, and CobIT is used to identify the actual control based on the control objectives concluded by using GAIT.

3.2 Applicability of GAIT to Sample Companies

It is understandable, that even though a new methodology has been released to attempt to increase efficiency and effectiveness of scoping, companies such as Companies A and B, would be hesitant to use it. They have, after all, gained experience and understanding on using CobIT. They have been able to use it in their companies, and through the years have reduced costs for compliance based on experiences and knowledge. Based on a survey completed by the Institute of Internal Auditors in

December 2007, many companies like Company A and Company B, who are past their first year of compliance, are still hesitant or would be hesitant to use GAIT because of issues their external auditors have or may have with it, as well as the fact that the company has already established and feel that they have optimized the controls structure using CobIT[21]. GAIT, however, can contribute largely to ensure that the control structure already developed, is effective in its control design, and efficient in control content. Since businesses change every year, the top-down risk based assessment should be conducted every year as well. This would involve the reassessing of materiality, significant accounts and major classes of transactions and then implementing the GAIT analysis. GAIT case studies on second year compliance companies have shown that by reassessing current control structures using GAIT, new business risks and control gaps have been identified and there has been an increased awareness between the IT and Finance departments of related controls[22].

As previously discussed, company A and B had a large reduction in the number of key controls they had in year three as compared to year one. One may ask whether there is a risk to lowering the number of controls. By removing a control, a company may feel that a risk is being exposed, however based on the fact that GAIT uses a top-down risk based approach, if a risk was to be identified, the process under which the risk falls would be identified early on in the top-down process. In addition, when assessing control risks, if the number of controls is lowered from previous years, the company must provide enough and appropriate documentation and reasoning for their basis on removing a control. GAIT provides a very detailed documentation process for control objectives

reasoning, through the various phases. This provides clarity for both the external auditors and internal auditors in understanding the reasoning for the removal of the control.

For first year companies, such as company C, GAIT can provide great benefits. Company C is currently following the full CobIT approach in order to assess their IT environment and business for the purposes of ICFR. This company can use GAIT to its full extent beginning with AS5's top-down risk based approach[23], identifying company level controls, identifying significant accounts and business processes. Once control objectives are determined, Company C can then use the CobIT 4.1 framework to identify controls from the objectives.

4.0 Conclusion

Different companies have differing complexities and differing business objectives. Frameworks and methodologies that have been available, have each provided their own guidance with regards to scoping ITGC's for the purpose of Section 404 compliance. CobIT and CobIT-lite is most widely used and as seen in this research, its use can be enhanced with the combination of the GAIT approach. The use of GAIT does not depend on the size of the organization. It is principles based and as such, can be used and defined for many different types of companies.

The key to ensuring that scoping of ITGC's is effective depends on a company's use of a top-down risk based approach. The top down assessment process results in the identification of critical IT functionality in financially significant applications. The top-down risk based approach is effective and efficient relative to quality and content of controls. The identification of significant accounts at the financial statement level drives the audit process down to the individual control level. GAIT continues this approach and

identifies the risks at the ITGC level. GAIT then goes on to recommend the use of the CobIT framework to identify and assess the controls. The use of three methods results in effective scoping. Effective scoping in turn can reduce the number of controls a company needs to test, if the company has already filed past its first year compliance as was seen with the sample companies. This reduces any costs related to these discounted controls. For those companies beginning on scoping ITGC's, GAIT provides a very flexible solution in terms of how they should go about scoping. Initial detailed work can save companies money on ITGC related costs in the long run when it comes time for testing.

5.0 Endnotes

[1] http://www.cfo.com/article.cfm/9033500.

[2] http://www.jeffersonwells.fr/Knowledge/pdf/pcaob_052407.pdf.

[3] PCAOB Accounting Standard 5; http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf, page 11.

[4] http://www.coso.org/publications/executive_summary_integrated_framework.htm.

[5] IT Control Objectives for Sarbanes Oxley, 2nd edition, September 2006; www.isaca.org/sox/.

[6] Ibid., page 9.

[7] Ibid., page 11.

[8] Ibid., page 3

[9] GAIT Methodology; Revised August 2007; www.theiia.org/download.cfm?file=83757

[10] New Scoping Methodology May ease Section 404 audits; January 2007;http://www.theiia.org/ITAuditArchive/index.cfm?iid=513&catid=21&aid=2501

[11]Scoping IT General Controls Executive Summary Report; January 2007; www.theiia.org/download.cfm?file=26790

[12] Names of companies are kept anonymous for reasons of confidentiality.

[13] IT Control Objectives for Sarbanes Oxley, 2nd edition, September 2006; www.isaca.org/sox/, page 99-100

[14] Benchmarking IT controls is where a specific ITGC's' assessment remains effective and a baseline on IT application controls has been established in prior years. Little work is needed.

[15] IT Control Objectives for Sarbanes Oxley, 2nd edition, September 2006; www.isaca.org/sox/, Page 27.

[16] Ibid.,

[17] GAIT Methodology; Revised August 2007; www.theiia.org/download.cfm?file=83757, page 8

[18] Ibid., page 16

[19] Ibid., page 19

[20] http://www.isaca-kc.org/doc/Gait.ppt#449,11,IT Risk Assessment and Scoping

[21] GAIT Executive Summary report December 2007; http://www.theiia.org/itaudit/iia-technology-updates/iia-technology-updates-1/, pages 4-5

[22] www.theiia.org/download.cfm?file=58891

[23] As shown in figure 4