

External ITGC Audits – *An Internal Auditor's Opportunity*

April 2, 2009

Presented to: The Dallas Chapter of the Institute of Internal Auditors

These slides are incomplete without the benefit of the comments made at the session. The information and considerations presented herein do not constitute legal or any other type of professional advice.

Today's Agenda

- Brief Overview of ITGCs
- Impact on Application Controls and System Generated Data
- Linkage to the Financial Audit
- Internal Audit Involvement in the ITGC Audit Life Cycle
- Additional Opportunities
- Final Thoughts

Questions to contemplate

- Have I contemplated Internal Audit's role in driving efficiencies in the external ITGC audit?
- Does the external auditor's ITGC budget seem high given the amount of work required?
- Am I doing everything I can to ensure the external auditors perform an efficient and effective ITGC audit?
- Have I been consistently interfacing with the external auditors during the planning, fieldwork and wrap up phases of the ITGC audit?
- Do the external auditors realize the maximum amount of reliance on my work? If not, what needs to happen to achieve maximum reliance?
- What else can I do to drive an efficient and effective ITGC audit?

Brief Overview of ITGCs

Entity Level Controls Over IT

- Relate to the “softer” COSO components
- ELCs should reflect how management approaches information technology needs and should serve to promote ongoing effectiveness of ITGCs
- Examples include:
 - IT Policies
 - Employee training
 - Communication
 - Adequacy of IT Team
- External Audit will assess the overall tone at the top to decide if the nature or extent of procedures should be modified.
- When past audits have indicated deficiencies in the control environment or relevant ITGCs and remediation efforts have been insufficient, the audit plan will be developed in consideration of the potential inability to rely on impacted automated controls.

ELCs over IT Set the Tone for controls in the organization.

ITGCs - What’s Relevant for Testing

- Access to programs and data
- Program changes

Both of these domains are almost always relevant, but their complexity and the extent of audit evidence needed can vary greatly by organization.

- Program development

Relevant only where new system implementations will impact ICFR and the risk of material misstatement. Testing generally not required if no impact on current year financial statements and ICFR.

- Computer operations

Relevant only if needed to directly address assertions over significant accounts (more common in high transaction volume industries with complex systems, such as banking) or to address specific risks.

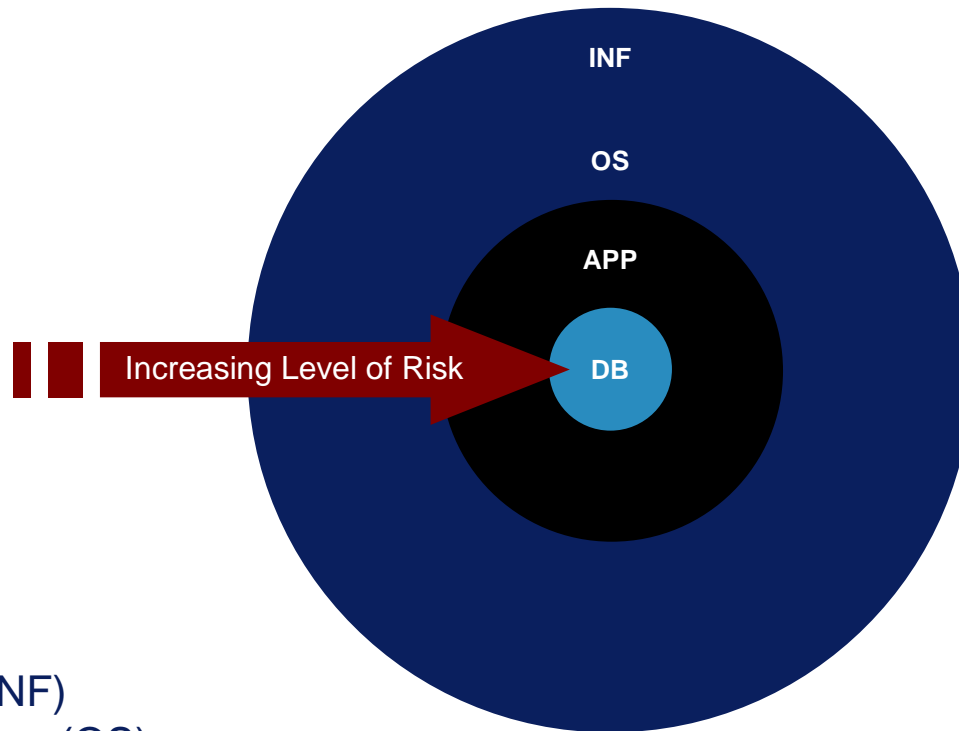
External Auditors will generally consider risks in each of these areas, even if little or no testing is performed.

ITGCs - Access to Programs and Data

- Areas for consideration:
 - Importance of restricted access to:
 - Segregation of duties objectives
 - Fraud risk
 - Risk of inadvertent errors
 - Company's approach to application security and the security infrastructure
 - Access (user and administrative) at the application, operating system and database levels
- It is usually not necessary to test perimeter security and anti-hacking controls, such as firewalls and intrusion detection systems, unless material financial reporting risks exist that are not adequately addressed by application-level security alone.

The closer you get to financial data, the greater the risk to material misstatement.

Layers of the Application Architecture and their Relative Risk



Infrastructure (INF)
Operating System (OS)
Application (APP)
Database (DB)

ITGCs - Program Changes

- Areas for consideration:
 - In house developed versus third party application
 - Ownership of source code
 - Volume / frequency of changes
 - Complexity of changes
 - Ownership of changes to key reports (business versus IT)
 - Where accountability sits in the organization for identifying changes impacting ICFR
 - Degree of finance and IT interaction

Forms the basis for relying on the ongoing operating effectiveness of application controls

ITGCs - Program Development

- Areas for consideration:
 - Methodology for implementing projects
 - Business involvement and buy-in on requirements and design
 - Contemplation of Internal Controls in design phase
 - Nature and extent of quality assurance (unit, regression, integration testing)
 - Accuracy and completeness of converted data
 - Go-live approvals

Not required to be tested unless there are specific data conversions or system implementations that impact the risk of material misstatement

ITGCs – Computer Operations

- Areas for consideration:
 - Job maintenance and monitoring (specific to financial jobs)
 - Backup and recovery procedures (in an unstable environment)
 - Operating system patch maintenance
 - Anti-virus controls
 - Environmental controls
- Computer Operations controls, otherwise not included in scope for the financial audit, are sometimes included in scope for the purposes of a statutory audit.

Often present operational risk, not ICFR risk, depending on the specific circumstances

Impact on Application Controls including System Generated Data

Application Control vs. an IT General Control?

- Application controls
 - Think in terms of “does this directly relate to the input, processing or output of financial transactions”
 - Directly support CAVR (Completeness, Accuracy, Validity and Restricted Access), thereby contributing to comfort over financial statement assertions
- ITGCs
 - Activities that ensure the *continued* effective operation of application controls, automated accounting procedures that depend on computer processes and manual controls that use application-generated information / reports
 - Some ITGCs may also serve as Application Controls, e.g. password controls
 - ITGCs are pervasive, and therefore often do not directly support financial statement assertions

Application controls include...

- Programmed or configured automated controls
- Reports or data generated from the system and used in manual controls or accounting procedures
- Automated calculations or data processing routines programmed into the application
- Restricted access to transaction processing capabilities
- Restricted access to programs and data
- ITGCs that directly address relevant financial statement assertions

Automated Controls - Baseline Approach

- A baseline test provides evidence that an automated control is functioning as intended at a point in time.
- ITGCs support a baselining approach:
 - If ITGCs are effective and continue to be tested AND an automated control hasn't changed since the last time it was tested then....
 - We can conclude the automated control continues to be effective.

The ability to rely on the proper and consistent operation of application controls usually depends on the effective operation of related ITGCs.

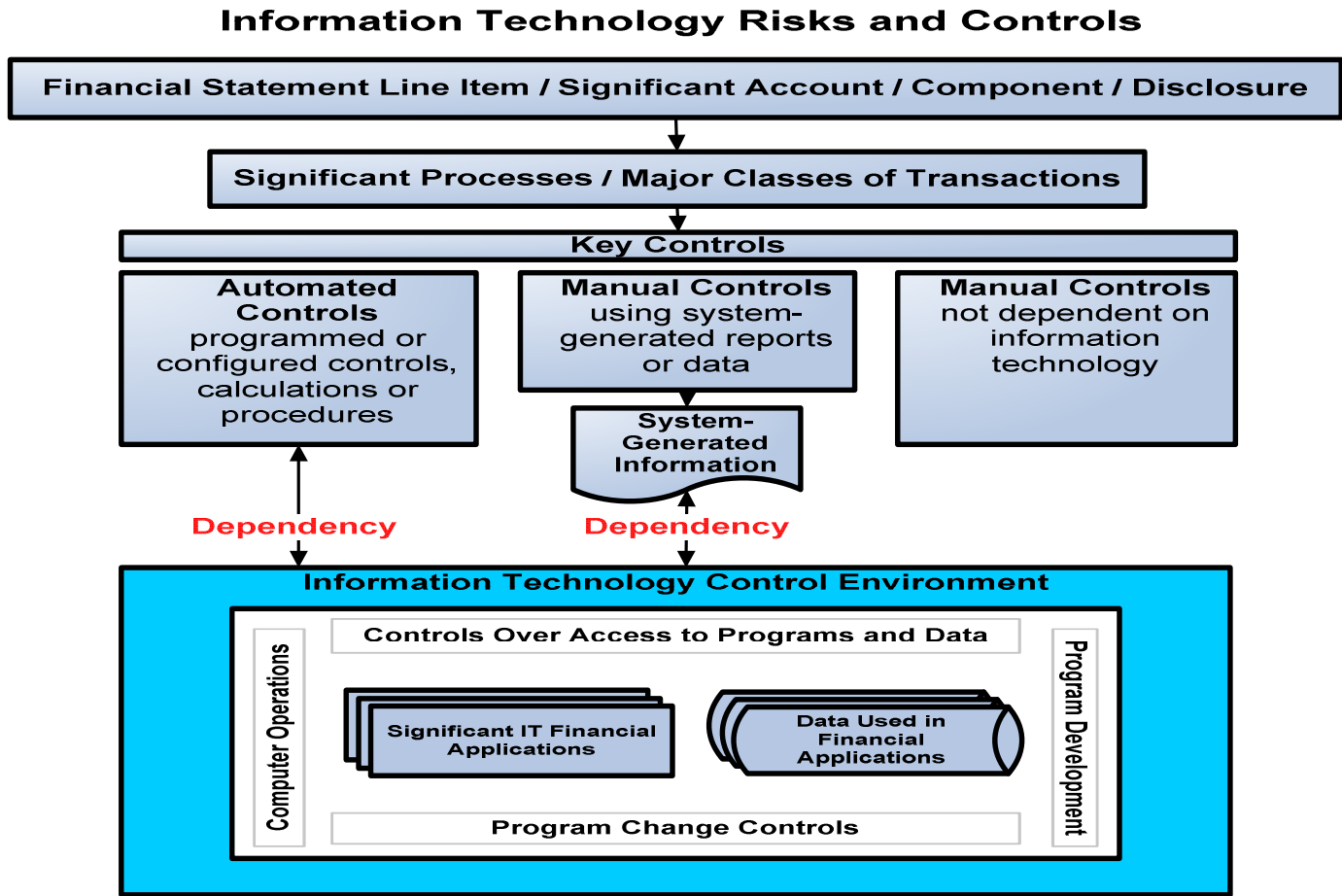
System Generated Data

- Often used in the execution of a manual control (ex: application generated reports)
- The higher the risk associated with the control and the more the control depends on the accuracy and completeness of data, the greater the importance of ITGCs
- Effective ITGCs provide greater comfort that the programs and data sources are controlled and protected from unauthorized access or changes

The ability to rely on the proper and consistent operation of application controls usually depends on the effective operation of related ITGCs.

Linkage to the Financial Audit

Linkage of ITGCs to Audit Comfort



Planning and Scoping considerations as it relates to the financial statement audit

- Overall scoping should be completed prior to planning for an evaluation of ITGCs
- ITGCs should be evaluated for those systems that have a direct linkage to the in-scope financial statement accounts considering relevant risk considerations
- Special consideration should be given when there are major system implementations
- Effective control design often includes a mix of automated controls and manual controls which rely on system generated reports
- Ensure approach is well coordinated between your IT auditors and the remainder of the team

Impact of ITGC deficiencies on the financial statement audit

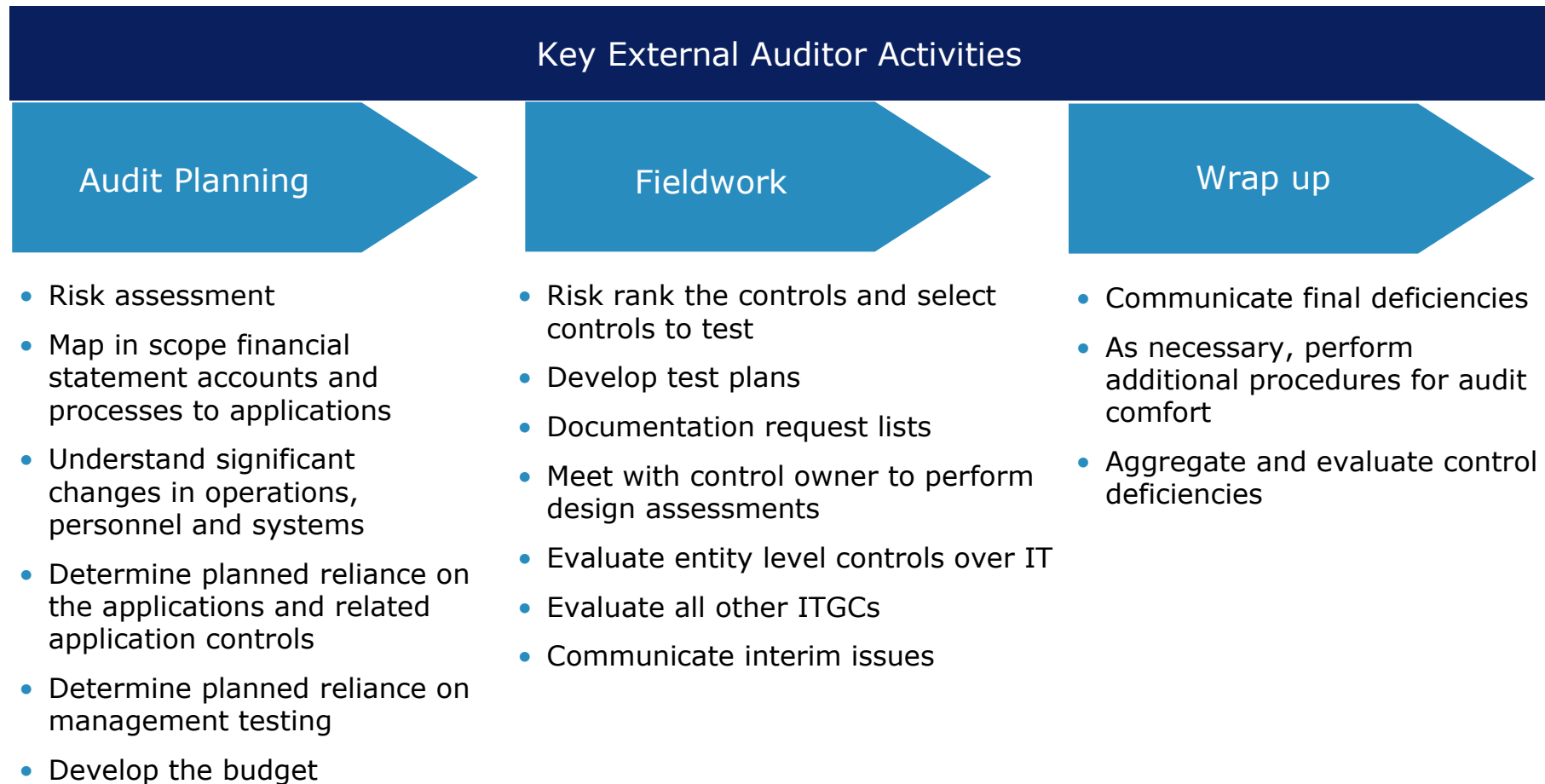
- ITGC deficiencies should be evaluated for their individual and collective impact on the reliability of the dependent automated application controls
- ITGCs should not be presumed to be ineffective because a few control deficiencies exist
- If the integrity of an automated control is impacted by an ITGC deficiency, determine whether the ITGC deficiency actually culminated in an application-level control issue

Evaluation of ITGC deficiencies requires integrated team judgment (both internal and external).

Internal Audit Involvement in the ITGC Audit Life Cycle

External ITGC Audits – *An Internal Auditor’s Opportunity*

To ensure efficiencies are maximized, Internal Audit teams should be involved in all three phases of the ITGC audit life cycle. Understanding the key activities for each phase is therefore critical.





Internal Auditor Opportunities during the Planning Phase...

- Read the SOX risk assessment/scoping memo to understand the financial statement risk; this may help you identify additional opportunities
- Risk rank the applications and controls
- Document and communicate competence and objectivity to the external auditors early
- Understand the external auditor's reliance approach and propose creative solutions to expand their reliance on management testing
- Document test plans early and submit to the external audit team for review

Develop a point of view and communicate it!



Internal Auditor Opportunities during Fieldwork...

- Validate deficiencies early via a combined effort between Internal Audit, External Audit and IT
- Provide management's workpapers timely and perform a thorough root cause analysis on any deficiencies found
- Clearly document Internal Audit's test procedures and results in a manner that facilitates efficient reliance by the External Auditors
- Communicate changes in your testing approach real time
- Understand the interim deficiencies and perform additional procedures to help the external auditors understand the exposure and any mitigating controls

Stay involved!



Internal Auditor Opportunities during Wrap-up...

- Always come with a point of view on deficiencies
- Understand differences in what management found versus your external auditors
- Anticipate and perform additional procedures resulting from ITGC deficiencies to help the external auditors understand the exposure and mitigating controls
- Aggregate and evaluate deficiencies via a defined framework (preferably one the external auditor uses)

Help drive management's deficiency evaluation to achieve greater reliance

Additional Opportunities

Additional Opportunities for Driving Efficiencies...

- Always think with AS5 (top down, risk based approach) in mind
- Be aware of upcoming changes in your environment that might impact ITGC scope, develop a point of view and bring to the table
- Risk rank the applications (in a complex environment with multiple apps)
- Enhance already existing SOX documentation (ex: ITGC narratives, scoping/planning memos, in-scope applications, SAS70s)
- Direct assistance (walkthroughs and/or testing)
- Pre and post implementation reviews

Develop a point of view on risk and support it with thorough documentation

Indicators of changes in the environment that might impact ITGC scope

- System implementation projects
- Data corruption / recovery issues
- Employee 'right-size' activities
- Outsourcing of functions previously performed internally

Final Thoughts

Questions?

Contact information

Dana Smith, Senior Manager

(214) 754-4583

Dana.Smith@us.pwc.com

Geoffrey Woodbury, Manager

(214) 754-5480

Geoffrey.S.Woodbury@us.pwc.com



This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2007 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP (a Delaware limited liability partnership) or, as the context requires, other member firms of PricewaterhouseCoopers International Ltd., each of which is a separate and independent legal entity. *connectedthinking is a trademark of PricewaterhouseCoopers LLP.