

COUNT ON INSIGHT<sup>SM</sup>



## Information Technology (IT) General Control Considerations and Implications

Presentation by: Jim Kreiser, Regional Director IT Advisory Services

October 20, 2011



## Overview

- Value of IT General Controls (ITGC)
  - Operational Benefits
  - Audit Enhancements
- ITGC Components & Key Areas
  - Logical Security
  - Change Control
  - Operations
- Leading Controls and Audit Procedures
  - Related Risks
- Impacts to Other Business Processes
  - Risk Assessments
  - ERM
  - Financial Audits and Reporting





## Why Evaluate IT Controls

- AICPA SAS Standards & Requirements
  - Risk Assessment Standards 104-111
  - “Eliminates the "default to maximum" for control risk, which should encourage testing of controls.”
  - SAS 94
- Influence of Sarbanes-Oxley (SOX) Within the Industry (Section 404 and PCAOB Standard AS2)
- Control based audit approach
- Better assessment of risk (control risk and IT risks) and entity-level controls



## What Are the Benefits?

- Improve Audit Efficiencies & Effectiveness
  - Reduce substantive testing
  - Mitigate unwarranted reliance
  - i.e. Reduce cost
- Improved Understanding of Controls and Financial Processes
- Better Communication of Risk and Control Environment
- May also add benefit of leverage with other regulatory reporting (i.e. FDIC, PCI, Legislative, A-133, etc.)





## Understanding IT Internal Controls

- Can we truly understand the financial reporting risks without evaluating the risks and impacts of IT controls and processes?
  - Report Integrity?
  - Misstatement risks?
  - Misappropriation of assets?
  - Fraud risks?
- Can we assess operational and organizational (ERM) risks without understanding the IT risk/Control risk?



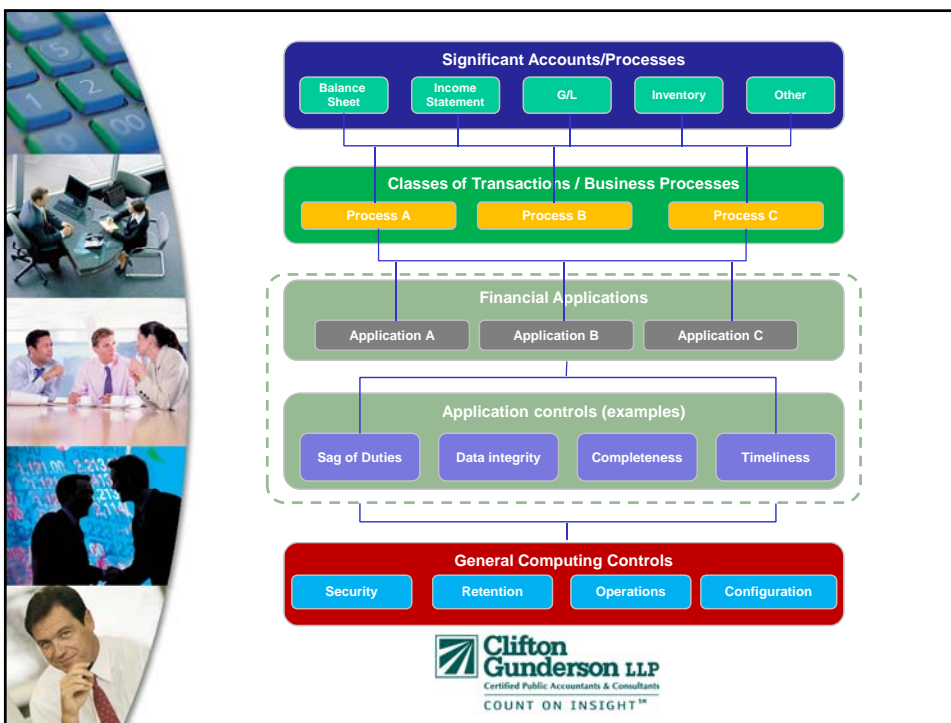
## Other Prevailing Factors

- PCAOB (Public Company Accounting Oversight Board)
  - Applies to SEC registrants
- FDIC (Federal Deposit Insurance Corporation) audit and control requirements
  - Currently references and is aligned with PCAOB guidance
- PCI (Payment Card Industry)
  - Data Security Standards
- Privacy and Regulatory Considerations
  - GLBA
  - HIPAA
  - BSA
- NAIC (National Association of Insurance Commissioners)
  - New requirements of non-profit and mutual insurance companies to report on internal controls (even non-SEC)
- Office of Management and Budget (OMB) A-123 and A-133 implications



# Types of IT Controls

- General Controls
  - Foundation Controls
- Application Controls
  - Operational Controls
- IT Dependent Controls
  - Reports





## ITGC Control Focus Areas

- IT Governance Controls
- IT Security Controls
- IT Operations Controls
- Development Controls
- Change Management Controls



## IT General Controls

- IT general controls are IT processes and related controls that are generally applied to support the computer application level. IT general controls are designed to:
  - Allow for changes to systems, databases, and applications to be properly authorized, tested, and approved before they are implemented
  - Allow for only authorized persons and applications to have access to data and perform specifically defined functions (e.g., inquire, execute, update).





## Why Test of Assess IT General Controls

IT General Controls (ITGCs) provide:

- The base of support for reliance on application and IT dependent manual controls (e.g., reports) related to the financially significant applications
- Basis for management assertions relative to monitoring, risk assessment and other audit & operational considerations

ITGCs Include:

- Logical Security, Change Control, and certain Operations controls (e.g., backup and recovery, job scheduling, physical/facility controls)

Effective ITGCs May Allow Us To:

- Perform a “test of one” for application and IT-dependent manual controls (e.g., reports)
- More accurately assess control risk, provide better ERM reporting, and support entity level control environments



## IT General Controls - Considerations

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>• <b>Logical Security Controls</b></li> <li>• Authorization of user access (internal and external)</li> <li>• Appropriateness of user rights</li> <li>• Segregation of duties</li> <li>• Security parameters in operating system</li> <li>• Password parameters</li> <li>• Security software settings</li> <li>• Security violation logging</li> </ul> | <ul style="list-style-type: none"> <li>• <b>Program Change Controls</b></li> <li>• Authorization and Approval of program changes</li> <li>• Testing/Quality Assurance</li> <li>• User involvement and sign-off</li> <li>• System Development Life Cycle (SDLC)</li> <li>• Source Code Control software – access restrictions &amp; version control</li> <li>• Emergency Changes approvals</li> <li>• Segregation of duties, including programmer access</li> </ul> |
|---|--|





## ITGC Operations

- **Backup and Recovery of Data and Programs**
  - Mechanism to track successful completion of backups
  - Population of backups
  - Periodic testing to establish the validity of backups
- **Incident Management**
  - Monitoring
  - Tracking and response
- **Job Scheduling**
  - May be governed by change control, but may also fall into operations
- **Physical/Environmental**



## Application Controls

- Application controls are automated processes that effect business transactions. There are two types of application controls:
  - Inherent to the application
  - Configured within the application
- Inherent controls include the Software logic defined by the software vendor (“Out of the Box Functionality”)
- Configured controls rely upon management to determine the parameters or possible values (e.g. tolerance levels in the Accounts Payable approval authority)





## Link of IT General Controls and Application Controls

In order to rely on, and utilize/assess, application controls, effective IT General Controls need to be present. Given that General Controls support Application controls, tests of both and effective conclusions of both are necessary for reliance.



## Application Controls

- Typical Application Examples
  - ERP Systems
  - Payroll Systems
  - Fixed Asset Systems
  - Spreadsheets
- Applications Are NOT
  - Operating Systems
  - Network Operating Systems
  - Utility Programs (Copy, Cut, Format, etc)





## Logical Access – Leading Controls

### Logical Security/Access

- Policies & Procedures
  - Minimum Security Baseline Standards
  - Acceptable Use Policy
  - Privacy/Confidentiality – e.g. Data Classification
- Processes
  - Restriction of Administrator (Root) functions
  - Single Sign-On or Pass Through Authentication(s)
  - Logging & Monitoring (Sysco)
- Organization
  - Segregate IT Security function
  - DBA review and separation from development/promotion
  - CIO Reporting – Aligned for entity overall?



## Logical Access Procedures & Risks

### Audit Procedures

- Validate appropriateness and approvals of user access
- Verify administrator access controls
- Review network and application account/password and audit policies (e.g. password syntax, intruder lockout, change intervals, etc.)
- Observe the performance of periodic access reviews

### Risks

- Evidence of network/application settings at a point in time. How to validate configurations over an extended period?
- Documentation. Are processes and review activities documented?





## Change Control

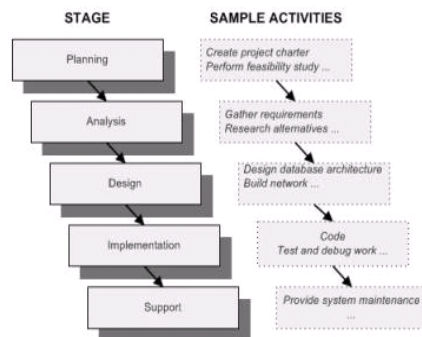
### Leading Controls

- Well defined and segregated development environments and promotion cycles
  - Test, QC, Model Office, Production
- Change Management “Committee”
  - Including version software or tools to notify/document migrations
  - Documented prioritization, review, and approval process
- System Development Life Cycle (SDLC)
  - Utilized for both in-house/custom applications and also for purchased software/systems
- Segregation of developers from operational IT team
- Implementation of automated approval tracking for changes
  - i.e. Endeavor, or other ticket systems such as Remedy



## SDLC Example Methodologies

**Waterfall** - A sequential design process in which process is seen as flowing steadily downward through the phases.



### Strengths:

- Easy to understand
- Highly structured
- Defined milestones
- Quality > Cost/Schedule

### Drawbacks:

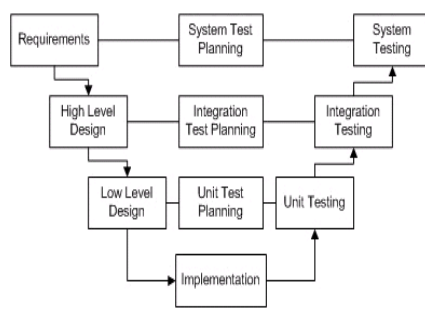
- Inhibits flexibility
- False impression of progress





## SDLC Example Methodologies

**V-Shaped** – An extension of the Waterfall method which demonstrates the relations between each phase of development and testing



**Strengths:**

- Easy to understand
- Emphasis on verification and validation
- Defined milestones

**Drawbacks:**

- Does not contain risk analysis activities
- Does not handle concurrent events
- Inhibits flexibility



## SDLC Phases

- Planning
- Requirements Definition
- System Design
- Implementation
- Verification and Validation
- Acceptance and Deployment
- Maintenance

*The project and change management function(s) may determine that all or only parts of the SDLC are applicable to the project. Guidelines should be included in the SDLC on how this decision should be made.*





## Change Control Procedures and Risks

### Audit Procedures

- Validate appropriateness of developer access
- Assess policy documentation of SDLC, change review and approval process, etc.
- Observe change migration and evidence
- Review configurations of version control and/or change approval tracking systems
- Test sample of changes for reasonableness

### Risks

- Identification of change populations. Often times there is manual tracking of changes, but limited evidence of system generated population of changes (i.e. may be limited to last executable change, etc.)
- How to assess or use judgment for approval process (i.e. emails, changes after-the-fact, etc.)?



## Operational Leading Controls

- **Backup and Recovery of Data and Programs**
  - Redundant operations, parallel processing and mirroring (virtual archiving/backup)
  - Archiving capabilities
  - Formalized data retention policies and procedures
  - Automated backup management system/logging
- **Incident Management**
  - Formal implementation of problem management/ticket system (including escalation, priority levels, etc.)
- **Job Scheduling**
  - Integrated scheduling system (e.g. Tivoli, OpenView, CA-Unicenter)
  - Shift turnover and job tracking mechanisms
- **Physical/Environmental**
  - Various, including facility redundancies, video surveillance, anti-passback, UPS, HVAC, etc.





## Operational Controls

### Risks

- Capabilities to assess facility controls such as:
  - Electrical redundancies
  - Sufficiency of UPS “modulation” of electric ebs/spikes
  - Sufficiency of HVAC implementations
  - Review of fire suppression coverage
- Ability to review/evidence over a period of time. Usually a point-in-time observation
- Validation of data disposal/retention – test strategies can be difficult.



## Other Implications of ITGCs

### Enterprise Risk Management Impacts

- Increases the ability of management and auditors to better dialogue and utilize concepts of control risk with greater assurance on judgments utilized
- Creates a better framework for the integration and evaluation of enterprise risks by adding a further component/criteria for the rating/assessment of other business and operations risks
- Increases the confidence and assurance of reporting related to risk reporting for the CIO, as well as the risk manager.
- Adds ability to more effectively assert and audit areas of IT risk for ERM in regards to any NAIC, FDIC, etc. standards, as well as potential internal reporting requirements (e.g. SSAE 16, A-133, etc.)





## Other Implications

### Audit Leverage

- Enhances the ability for auditors to leverage entity level control considerations to lower risk assessments and use control testing within the audit approach
- Provides better internal reporting and evidence for external or internal audits to lower risk assessments relative to auditable units
- Supplies better evidence, documentation, and analysis to support compliance reporting requirements.
- Allows for negotiations with external audits on costs and effort due to the ability to have an expanded controls based audit approach and flexibility in the audit approach (if ITGCs are effective/mature)



## Other Considerations

- Various systems, platforms, utilities, interfaces, and applications greatly impact the shape and context of the ITGC environment.
  - Several systems and applications have limitations relative to logical access security features
  - Applications, operating systems, and databases may or may not integrate well and/or perform optimally from an ITGC capability perspective
  - Platforms used will greatly impact decisions and determinations relative to ITGCs
  - As with most other internal control aspects, there is a “balancing act” relative to managing the cost of implementing tools/applications to enhance ITGC vs. managing the level of risk tolerance that the organization will accept
  - The use of spreadsheets, ODBC, and other similar data file types makes the implementation of ITGCs more complex and difficult. “Operationalizing” data and reporting where possible generally enhances the control environment



## Summary

- IT General Control Benefits:
  - Improved knowledge and understanding of management processes and control environment
  - Reduced substantive testing of reports and transactions
  - Reduced/eliminated testing of manual controls or manual tests of controls
  - Better communication and feedback to management of control/process improvements (i.e. use of application controls, control gaps, spreadsheets, etc.)
  - Reduced audit risk, and reduced risk of unwarranted reliance (i.e. better audit coverage)



## QUESTIONS?

