IT Controls and Audit Procedures

Presentation by: Josh Coakley and Phil Del Bello

April 14, 2022

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Learning Objectives

At the end of the session, you will be able to:

- Identify methods utilized by IT audit to evaluate IT security based on general control concepts.
- Identify how to apply techniques and procedures to evaluate controls over the IT environment.
- Recognize potential weaknesses in IT general controls.

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 Audit IT Controls

- IT systems support many (if not all) business processes
- Cannot rely on IT systems or the data without effective IT controls
- Standards required IT controls to be implemented
  - AICPA SAS Standards & Requirements
  - 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
  - Completeness, Accuracy, Validity, Authorization
- 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.)

Scoping an IT Audit

- Multiple application systems, data warehouses, report writers, and layers of supporting IT infrastructure (database, operating system, and network) may be involved in the business process
- The classes of transactions
- Procedures, within both automated and manual systems, by which those transactions are initiated, authorized, processed, recorded, and reported
- Ways in which the information system captures transaction

Performing and IT Audit

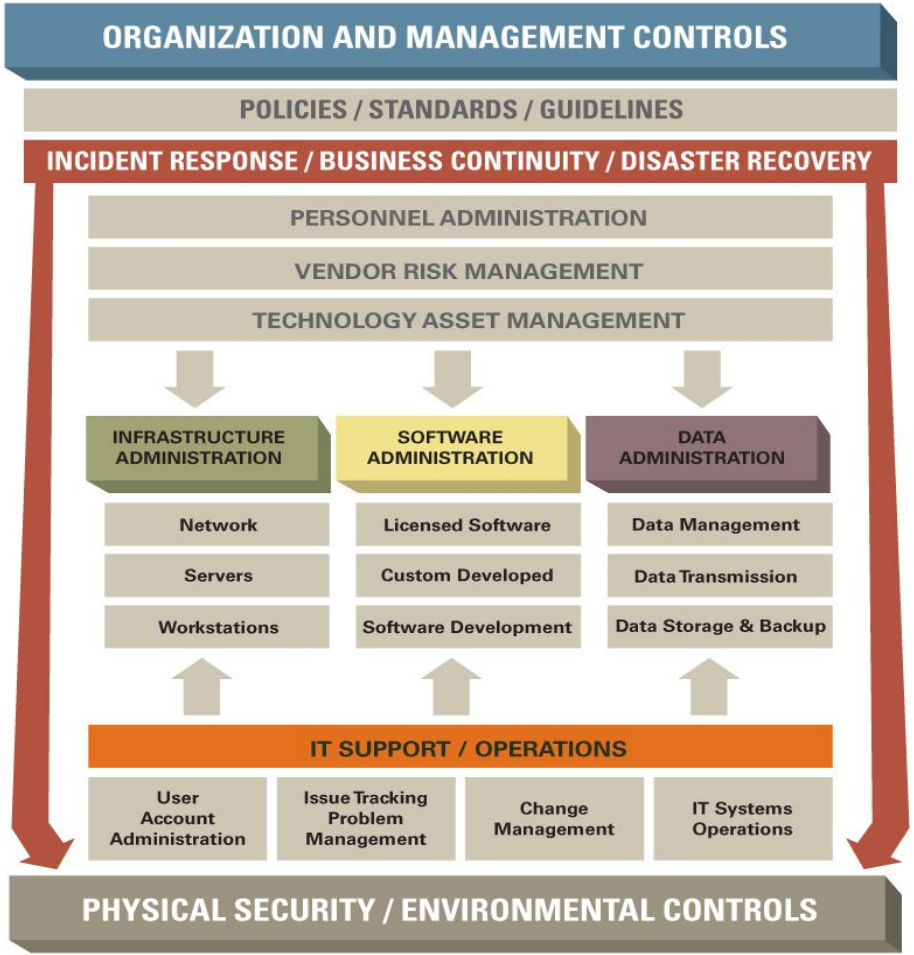
- Understand and identify the IT environment
- Conduct interviews, walkthroughs, and test of documentation
- Assess design of existing controls
- Assess control operating effectiveness
- Automated tools used for scanning and auditing
- Reporting

IT Controls Testing

Types of IT Controls

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

- Control Types
  - Automated
  - Manual
  - Partially Automated
  - Preventive
  - Detective
  - Corrective



IT General Controls

- IT processes and related controls generally applied to support the computer application level

- Control purposes:
  - Changes to systems, databases, and applications
    - Authorized, tested, and approved before they are implemented
  - Authorized persons and applications
    - Access to data and perform specifically defined functions

Why Test to Assess IT General Controls

IT General Controls (ITGCs) provide:

- The base of support for reliance
- Basis for management assertions

Effective ITGCs May Allow Us To:

- Perform a “test of one” for manual controls
- More accurately assess control risk
- Provide better ERM reporting
- Support entity level control environments

IT General Controls - Considerations

- Governance
  - Policies and procedures
  - Roles and responsibilities
- Logical Access
  - User access provisioning / de-provisioning
  - Administrator access
  - Authentication process
  - Access recertification
- Computer Operations
  - Batch job processing
  - Interface monitoring
  - Backup and recovery
  - Incident handling
- Change Management and Software Development
  - Authorization, development, testing, approval, implementation
  - Production vs test environment
  - Emergency changes
  - Configuration changes
  - Patch management

Logical Access

Logical Access – Governance

- Policies & Procedures
  - Minimum Security Baseline Standards
  - Acceptable Use Policy
  - Privacy/Confidentiality – e.g. Data Classification

- Roles and Responsibilities
  - Business unit management is included in the IS function from a data ownership perspective
  - Segregate IT function of administering access from Business Unit function of owning the data

Logical Access – Provisioning

- Access rights been defined and established by appropriate levels of IT

- Consider access to:
  - Applications
  - Application data outside applications
  - Operating system

- Access rights are properly granted, changed and removed
- Develop role-based access for manageable processes

Logical Access – Access Review

- Periodically review application, operating system, and database access
- Can be facilitated by IT to obtain the data
- Responsibility should be the “owner” of the application or data
- Include all active users and detailed permissions

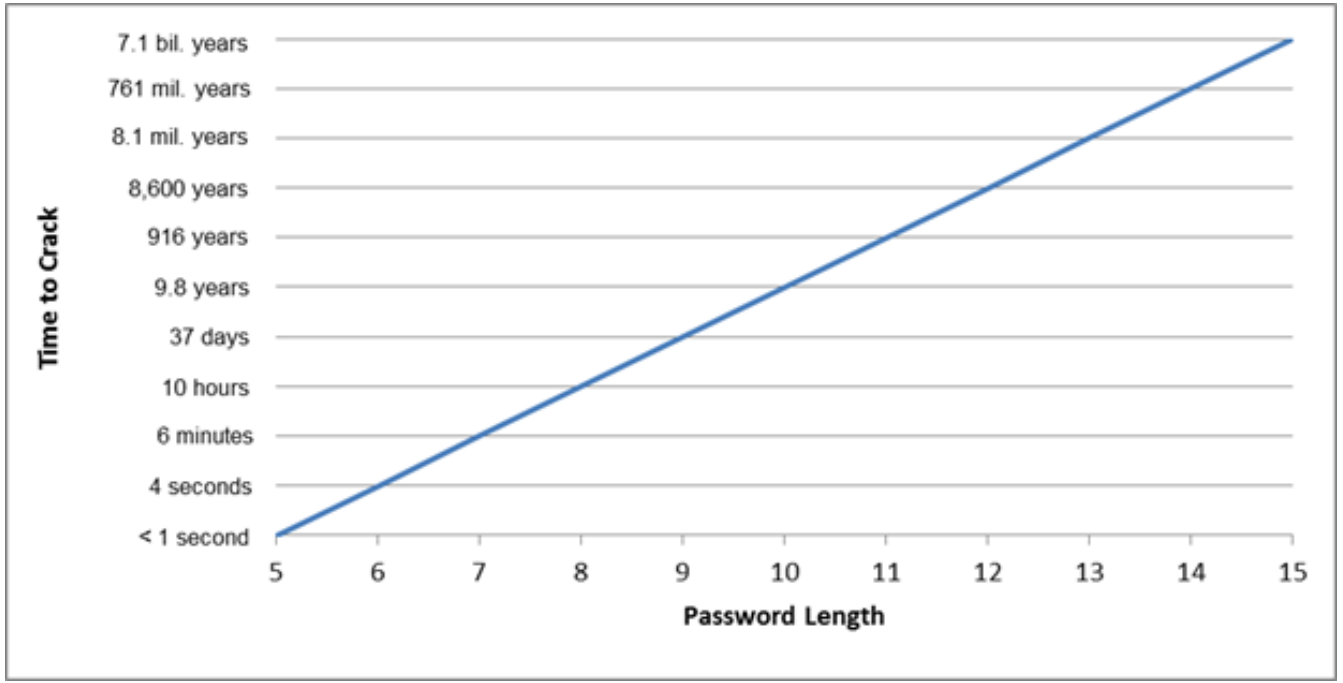
Logical Access – Administrator Access

- Restrict Admin/Super User/Root access to the least number of individuals
- Two accounts – 1 for everyday use and 1 for admin functions
- Monitor the environment for potential unauthorized activity

Password Configuration Testing

- Password Characteristics
  - Length and complexity
  - Longer passwords are harder to guess or crack
- Password History
  - Users should not be allowed to reuse a password
  - Setting should prevent reuse for as long as possible
  - Critical to communicate to users not to use the same password for everything
- Account lockout
  - Shorter lockout = More calls for password reset
  - Longer lockout = mor attempts to crack a password

Time to Crack



This represents raw brute forcing the entire keyspace (no wordlists) a single Windows password in NTLM hash format. This is based on our password cracking server which has 8 GPUs (can crack 1.75 billion NTLM hashes per second).

Remote Access – Multi-Factor Authentication

- MFA required on any type of remote access or cloud apps
- Ensure the connection is secure (VPN, TLS 1.2, Encryption)
- Restrict remote access to only those needed timeframes (business hours or current network time restrictions)

New User Access Testing

- Determine your population
  - HR list of New Hires
  - Compare current year access list with prior year access list
  - For testing a specific application, compare HR list with current access list
- Determine that documentation exists for:
  - Who requests/initiated the access
  - Who approved the access
  - Who implemented the access
  - Current access matches the requested/approved access

Termination Testing

- Determine your population
  - HR list of terminated individuals
- Test of Termination Control:
  - Who requests/initiated the access removal
  - Who implemented the access removal
  - Ensure all access that was requested historically has been removed
  - Determine access was removed timely
- Substantive Test of Termination
  - Compare listing of all terminations during a period with active user listing

Change Management

Change Management

Goals

- Limit the introduction of faults into the system
- Minimal interruptions to services while maintaining cost effective utilization.

Leading Controls

- Well defined and segregated development environments and promotion cycles
  - Test, QC, Model Office, Production
- Change Management “Committee”
- System Development Life Cycle (SDLC)
- Segregation of developers from operational IT team
- Implementation of automated approval tracking for changes

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
- 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
- How to assess or use judgment for approval process

Change Management Testing

- Determine the population
  - The change population can be difficult to identify
  - Using a list of all tickets for changes is not a population
    - Those tickets are the changes that followed the process
    - Goal is to identify if any did not follow the process
  - Database log of version history
  - Source code merged to production branch
  - Listing from vendor or all releases available

Change Management Testing

- Key Controls
  - Prioritization and classification of changes,
  - Authorization of changes at various stages,
  - Testing requirements and associated documentation requirements,
  - Requirements/approval for move to production, and
  - Requirements for post-implementation review.

Change Management – Testing

- Structured approach to testing based on the use of test plans
  - Exhaustive checking of the individual programs and of the entire system.
  - System will process valid data correctly but reject invalid data
  - Documented test plans
    - Test cases / scenarios, test conditions, expected test results and test criteria.
  - Test plans include sufficient detail to allow for comprehensive testing
  - Test results should be documented and compared against expected results
    - Any discrepancies should be highlighted for further investigation
    - If necessary, the appropriate program changes should be made and re-tested.
  - Test plans should be signed-off by IT management and retained for audit review
  - If packages are being tested, evidence should be obtained from the vendor

IT Operations

IT 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

Operations Leading Controls

- Backup and Recovery of Data and Programs
  - Redundant operations, parallel processing and mirroring (virtual archiving/backup)
  - Data recovery testing
  - 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 and monitoring system
  - Shift turnover and job tracking mechanisms
- Physical/Environmental
  - Various, including facility redundancies, video surveillance, anti-passback, UPS, HVAC, etc.

Application Controls

- Application controls are automated processes that affect 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 Control Examples

- 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.)

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, ODBCs, 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

QUESTIONS?

Thank you!

Joshua Coakley
Joshua.Coakley@CLAconnect.com

Phillip Del Bello
Phillip.DelBello@CLAconnect.com

CLAconnect.com

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING