Effective Controls over Information Security… An Auditor's Perspective

Vlad Liska
Project & Consulting Manager, Corporate Audit
TD AMERITRADE Holding Corporation

August 22, 2008

"Good controls reveal problems early, which means we'll have longer to worry about them." - Mike Harding Roberts

TD AMERITRADE Holding Corporation

Introduction

- Internal Controls Overview
- Internal Audit's Role
- Information Security Controls
- Physical Security Controls
- Summary / References
- Questions / Comments

Internal Controls Overview

"A policy, procedure, practice, or organizational structure designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected."

– CobIT 3rd Edition

Internal Controls Overview (continued)

- Controls prevent “bad” things from happening and enable businesses to do business
  - Examples

Internal Controls Overview (continued)

- Internal control is a process
- Internal control is effected by people
- Internal control provides only reasonable assurance
- Internal control is focused on achievement of objectives by addressing risks

Internal Controls Overview (continued)

FORMAL	INFORMAL
Policies and Procedures	Values / Culture
Authorizations	Attitudes
Reconciliations	Integrity
Verifications	Commitment
Dual Control	Understanding
Segregation of Duties	Knowledge / Competence
Documentation	Trust
Reviews	
Accountability	

Internal Controls Overview (continued)

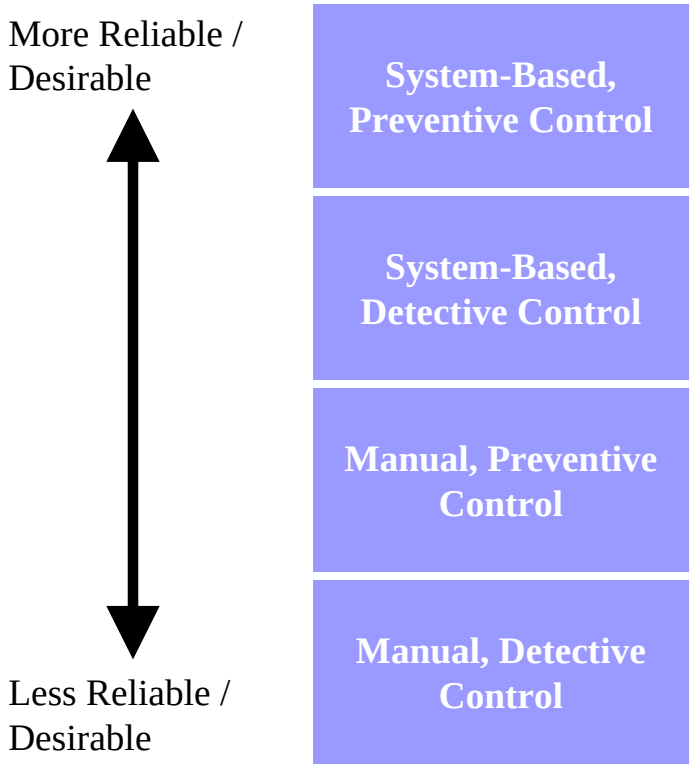
- Preventive Controls - Designed to prevent errors or omissions from occurring and are generally positioned at the source of the risk within a process
  - Example
- Detective Controls - Designed to detect and correct an error or fraud within a timely manner prior to completion of a stated objective
  - Example

Internal Controls Overview (continued)

- Manual Controls - Depend upon the manual execution by one or more individuals
  - Example
- System Controls - Depend upon programmed application or IT systems to execute a step or perhaps prevent a transaction from occurring without manual decision or interaction
  - Example

Internal Controls Overview (continued)

- A proactive approach to controlling risk requires greater use of preventive controls than the reactive “find & fix” approach embodied in a detective control.
- Systems-based controls are often more reliable then people-based controls because they are less prone to mistakes.



TD AMERITRADE Holding Corporation

Internal Audit's Role

- Internal Audit must determine that the established systems of internal control are complete, reliable, efficient, and effective. Properly designed system of internal controls will:
  - Support management's decision making processes
  - Safeguard assets
  - Ensure compliance with significant laws and regulations
  - Ensure reliability and integrity of corporate records and information systems

Internal Audit's Role (continued)

- Not my problem?
  - Five of the seven largest bankruptcies in history followed annual reports with clean audit opinions (Bloomberg)
  - In more than half of the 673 largest bankruptcies of public companies since 1996, auditors provided no cautions in previous annual financial statements (Institute of Internal Auditors)
  - In the past five years, one in 10 publicly traded companies in the United States had to reissue its financial statements after accounting irregularities were discovered (Institute of Internal Auditors)
  - Sarbanes-Oxley

Information Security Controls

- General Computer Controls
  - Application Development, Change Control, Operations, and Information Security
- Information Security Controls
  - Management & Roles / Responsibilities
  - Awareness & Training
  - Incident Monitoring
  - Logical Security (all levels)
  - System Administration
  - Networking
  - Vendor Management

Information Security Controls (continued)

- **Overall Security Management (policy)**
  - Management should establish information security policies, which are based on the level of risk arising from access to programs and data.

- Effective Controls
  - Documented, approved, and communicated security policy
  - Regular review and update process
  - Defined exception process

Information Security Controls (continued)

- **Setting Roles, Responsibilities and Procedures**
  - Management should establish appropriate roles and responsibilities for information security, and ensure that those with responsibility follow appropriate procedures.

- Effective Controls
  - Defined roles and responsibilities
  - Detailed procedures (document, approved, and communicated)
  - Standard hardware configurations
  - Compliance monitoring processes

TD AMERITRADE Holding Corporation

Information Security Controls (continued)

- **Security Awareness Education and Training**
  - Management should ensure users receive appropriate education and training on information security so that they understand the issues, the organization's policies and the actions they are expected to take.

- Effective Controls
  - Employee orientation and sign-off (disciplinary actions)
  - Ongoing security awareness and training program (classes, newsletters, posters)
  - Periodic assessments (surveys, social engineering testing)

Information Security Controls (continued)

- **Monitoring Security Incidents**
  - Management should monitor security incidents and execute appropriate procedures to minimize the negative impact.

- Effective Controls
  - Implemented and monitored network IDS
  - Proactive vulnerability identification and management
  - Logging and timely review
  - Defined escalation and communicate processes

Information Security Controls (continued)

- **Administering Logical Security at OS Level**
  - User access to the computer operating system and programs should be appropriately restricted.

- Effective Controls
  - Basic password controls
  - Limit world-writable files / world-writable directories
  - Audit trail reviewed
  - Restrict command line access
  - User account management

Information Security Controls (continued)

- **Administering Logical Security at the Database**
  - Access to data should be appropriately restricted.

- Effective Controls
  - Data views restricted based on need
  - User account management

Information Security Controls (continued)

- **Ongoing Security Administration within Applications**
  - Appropriate facilities and procedures should be in place to manage access to particular functions within systems and support the restriction of access to ensure segregation of duties and prevent unauthorized activity.

- Effective Controls
  - Application controls
  - Group based security
  - Application audit trail
  - User account management

TD AMERITRADE Holding Corporation

Information Security Controls (continued)

- **System Administration and Privileged Accounts**
  - Use of sensitive facilities, such as master passwords, powerful utilities, and system manager facilities, should be adequately controlled.

- Effective Controls
  - Passwords changed frequently
  - Default passwords changed
  - Limit generic user-ids
  - Usage of system administrator accounts logged

Information Security Controls (continued)

- **Controlling Network and Dial-up Access**
  - Remote access to computer systems (via network connections or dial-up) should be appropriately restricted.

- Effective Controls
  - Multi-factor authentication
  - Limit trust relationships
  - Restrictions to appropriate times of the day / week
  - User account management

Information Security Controls (continued)

- **Controlling Network Connections**
  - Network connections should be used for valid business purposes only and controls should be in place to prevent these connections from undermining system security.

- Effective Controls
  - Network segmentation (firewalls)
  - Secure transmissions (encryption)
  - Comprehensive penetration testing
  - Change control process over network devices and rules

Information Security Controls (continued)

- **Vendor Management**
  - Appropriate safeguards should be in place to ensure assets are protected from vendor threats.

- Effective Controls
  - Executed non disclosure agreements
  - Risk based security review process (questionnaire, site visit)
  - Periodic re-review process

Physical Security Controls

- **Physical Security**
  - Physical access to computer facilities and data should be appropriately restricted.

- Effective Controls
  - Physical access to the site / building restricted
  - Physical access to the computer room restricted
  - Clear desk policy
  - No public signs
  - Secure disposal of discarded computer equipment and media

Summary

- Security Controls
  - Documented controls
  - Reasonable assurance
- Management review
- Self testing of controls
- Independent evaluation of controls

TD AMERITRADE Holding Corporation

References

- CobIT – Control Objectives for Information and Related Technologies
  - http://www.isaca.org
- COSO – The Committee of Sponsoring Organizations of the Treadway Commission
  - http://www.coso.org

Contact / Questions / Comments

- To contact me
  - Vladimir.Liska@tdameritrade.com
  - Tel. 402-827-8684

- Questions / Comments

Thank you for attending!