Information Technology General Controls and Best Practices

1. IT General Controls - Why?
2. IT General Control Objectives
3. Documentation Practices
4. IT General Controls
5. Top 10 Common Deficiencies
Paul Perry has been with Warren Averett since 2004 and is a Senior Manager in the Security and Risk Consulting Division of Warren Averett Technology Group – focusing on internal control and information technology related projects.

Paul is also a member of the Firm’s Data Analysis Group, a team of individuals within the Firm who provide data analysis solutions to both internal and external clients.

For a number of years, he has specialized in accounting advisory and review assurance services, as well as external and employee benefit plan audits. Paul has extensive experience serving clients in the nonprofit, governmental, financial, insurance and healthcare facilities/hospital industries.
Warren Averett – Firm Facts

SIZE OF FIRM
850+ employees

OFFICE LOCATIONS
15
ALABAMA
Anniston
Auburn
Birmingham
Cullman
Foley
Huntsville
Mobile
Montgomery

FLORIDA
Destin
Fort Walton Beach
Pensacola
Tampa

GEORGIA
Atlanta

AFFILIATE COMPANIES
6
> Warren Averett Asset Management
> Warren Averett Benefit Consultants
> Warren Averett Staffing & Recruiting
> Warren Averett Technology Group
> Warren Averett Turnaround Advisors
> Warren Averett Workplace

AFFILIATE OFFICES
Houston
Grand Cayman

RANKINGS
2
Largest CPA firm among Gulf Coast states

4
Largest CPA firm in the Southeast/Gulf Coast combined

27
Largest CPA firm in the U.S.

CLIENT OPERATIONS
50 states
36 countries outside the U.S.

MEMBERSHIPS
4
> AICPA Major Firms Group
> BDO Alliance USA
> PCAOB
> Redstone Government Consulting Alliance

Source: Accounting Today 2015
IT General Controls – Why?

Key Risk Areas

- Financial
- Operations
- Information Systems

Sample Risk Assessment Types

- Financial Risk Assessment
- Compliance Risk Assessment
- Fraud Risk Assessment
- Cyber Risk Assessment
- Customer and Credit Risk Assessment
- Supply Chain Risk Assessment
- Product Risk Assessment
- Strategic Risk Assessment
Information Technology General Controls

COSO Model of Controls

[Diagram of the COSO Model of Controls]

[Logo: Warren Averett CPAs And Advisors]
IT General Control Objectives

1. STRUCTURE AND STRATEGY
   Evaluate if reasonable controls over the Company’s Information Technology structure are in place to determine if the IT Department is organized to properly meet the Company’s business objectives.

2. CHANGE MANAGEMENT
   Evaluate if reasonable controls are in place over change management relative to the operating systems and network environment to determine if standard maintenance changes (e.g. patches, fixes, upgrades, etc.) are identified, approved, and tested prior to installation.

3. VENDOR MANAGEMENT
   Evaluate if reasonable controls are in place over third-party services to determine if third-party services are secure, accurate and available, support processing integrity, and are defined in performance contracts.
IT General Control Objectives (Continued)

4. SYSTEM & APPLICATION SECURITY
   Evaluate if reasonable controls are in place over system security, both logical and physical, to determine if software applications and the general network environment are reasonably secured to prevent unauthorized access and appropriate environmental controls are in place.

5. INCIDENT MANAGEMENT
   Evaluate if reasonable controls are in place over incident management to record, investigate, and resolve any user or system incidents and management monitoring of system incidents exists.

6. DATA MANAGEMENT
   Evaluate if reasonable controls are in place over the data management and storage process (backups and disaster recovery) and are being tested on a regular basis.
Information Technology General Controls

**DOCUMENTATION**

- Who performs what?
- In what order are the controls performed?
- How often are they performed?
- Titles and not specific personnel. Personnel change.

**Key and Non-Key Controls**

- Need a good mix of both
- Non-key – process controls (how something is done and documented)
- Key – review controls (who reviews what others have done or major controls – without this, something cannot be done)
- Can be manual or automated

“If it is not documented, you did not do it”
Information Technology General Controls

Preventive – Detective – Corrective

- **Preventive** – prevent problems from occurring (Proactive)
  - Segregation of Duties
  - Monitoring
  - Adequate Documentation
  - Physical safeguards

- **Detective** – identify problems after occurrence (Reactive)
  - Data Analytics
  - Reviews
  - Monitoring

- **Corrective** – prevent recurrence of problems
  - Revisit the risk assessment process
  - Change controls as needed to eliminate error in future.
Information Technology General Controls

1 - STRUCTURE & STRATEGY

- Overall IT governance
- IT Strategy
- IT Steering Committee
  - Are others involved outside IT (HR, C-Suite, etc.)
- Business Processes and Owners of Key Systems
- Structure of IT department
  - Separate Security Department (sole focus on overall security)
2 - PROGRAM CHANGE MANAGEMENT

• Change management policies and procedures
• Segregation of duties
• Separate test environment
• Testing over change process
  • Authorization
  • Testing
  • Documentation
• Change management over operating systems and the network
  • Review on periodic basis to baseline
• Database change management
3 - **Vendor Management**

- Vendor management policies
- Vendor listing and risk assessment
  - Vendor Questionnaire
- Reviewing SSAE 16 (Service Organization Control) reports for vendors with access to clients' network or holding clients' data.
Information Technology General Controls

4 - System & Application Security

- IT risk assessment
  - Organization-wide or IT Specific
- Security policy and IT policies and procedures
  - Acceptable Use Policy
- Network and financial application administrators
  - Shared accounts limited
- Network and financial application password parameters
  - UC/lc and Alphanumeric
  - > 8 Characters
  - Changed every 90 days
  - Remember last 5 logins
  - Failed attempt lockout (3 attempts) – monitoring/logging
  - Inactivity logout (15 mins)
Information Technology General Controls

4 - System & Application Security - Continued

- New hire and termination process
  - Requests and approvals for access to different systems
  - Acknowledge IT Acceptable Use Policy
  - Notifications of terminations
  - Termination checklist
- Local administrator access
- Logical access review
  - Periodic (quarterly or annually)
  - Who is reviewing – IT or department managers
- Unsupported versions of operating systems and software
- Firewall policies and administrators
  - Reviewed periodically
  - Updated with current technology
Information Technology General Controls

4 - System & Application Security - Continued

• Intrusion Prevention and Detection Systems
  • Detect, log and analyze
  • Identify incidents or potential incidents
  • Prioritize based on impact
  • Track and status of incidents
  • How often are reports reviewed – consistently or weekly?
• Content and Spam Filtering Systems
• External penetration test and internal vulnerability scans
  • Periodic (quarterly or annually)
  • All IP addresses should be scanned
• Anti-virus monitoring and logging
  • Remediation if items slip through
Information Technology General Controls

4 - System & Application Security - Continued

- VPN administrators
  - Shared Accounts?
- VPN Dual Factor Authentication
  - Password and company owned device or mobile phone
- Policies and access controls over portable devices
  - Acknowledged by employees?
- Encryption on portable devices
  - Ability to wipe remotely?
- Annual IT Security Training for all employees
  - Document who attended and what was communicated
- Physical access and environmental controls over the Computer Facility/Data Center
  - Does entire organization have access or just IT department
Information Technology General Controls

5 - INCIDENT MANAGEMENT

• System monitoring policies and procedures
• System monitoring alerts
• Help Desk policies and procedures
• Help Desk monitoring reports
Information Technology General Controls

6 - DATA MANAGEMENT

- Data distribution policies
- Secure File Sharing
- Back-up policies and procedures
  - Include record retention policies for different types
  - Daily – 14 days, Monthly – 6 months, Annual – 7 years
- Back-up monitoring logs
- Restoration of back-up files
  - Tested on regular basis
- Physical security over back-up tapes
  - Transport log maintained
- Encryption of data backups
- Disaster recovery plan
- Disaster recovery testing – all systems vs critical applications
Top 10 Common Deficiencies

1. Terminated employees still active in systems and the network
2. Lack of segregation of duties over the development and production environment
3. Lack of critical application list – no knowledge of vulnerabilities
4. Lack of vendor management program and no vendor risk assessments
5. Lack of external penetration testing and internal vulnerability scanning – cost or understanding
6. Shared and/or generic administrator accounts without monitoring
7. Weak system password parameters
8. Outdated disaster recovery plan and no testing completed (financial applications and full IT network)
9. Lack of data backup testing
10. Lack of portable device policy and security
QUESTIONS?

Paul M. Perry, FHFMA, CITP, CPA
paul.perry@warrenaverett.com
(205) 769-3251
CPAs AND ADVISORS

LET’S THRIVE TOGETHER