Right-Sizing IT Audits for Small and Mid-Sized Enterprises

Robert Fleming CISA, CIA, CFSA
IT Principal/Partner
Simpson and Simpson, CPAs
Direct (213) 873-5923
rfleming@simpsponandsimpsoncpas.com
Why The Need To Scale Down or Adjust Procedures For IT Audits of Small To Mid-sized Enterprises?

Some factors to consider:

- Complexity and size of IT operations (e.g., number of servers)
- Complexity of information systems (e.g., SAP vs. QuickBooks)
- Number of users that accesses network and accounting systems
- Volume of accounting transactions processed
- Number of application and infrastructure changes processed
- Size of IT staff
- Etc.
How Do Some Classify Small and Mid-Sized Companies?

<table>
<thead>
<tr>
<th>Company Size</th>
<th>Revenue</th>
<th>IT Budgets</th>
<th>IT Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>$5 mm to $50 mm</td>
<td>$350,000 - 3.5 mm (6.9% of revenue) *</td>
<td>1 – 10</td>
</tr>
<tr>
<td>Mid-Sized</td>
<td>$50mm to $500 mm</td>
<td>$2.05 mm – 20.5 mm (4.1% of revenue) *</td>
<td>10 – 100</td>
</tr>
</tbody>
</table>

*Source: SearchCIO*
Benefits of IT Audit

- Can reduce overall audit effort; e.g., reduce substantive testing
- Deliver comments to improve client’s system security, integrity, availability and cost control
- Help client optimize IT processes
- Increase audit efficiency and profitability
## Key Challenges for Small and Mid-Sized Companies

<table>
<thead>
<tr>
<th>Factors that Impact Implementing Internal Controls</th>
<th>Why?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of Segregation of Duties</td>
<td>Smaller Number of Personnel</td>
</tr>
<tr>
<td>Limited staffing</td>
<td>Cost (e.g., salaries)</td>
</tr>
<tr>
<td>Competency of personnel</td>
<td>Scale of Operations</td>
</tr>
<tr>
<td>Tone at the top</td>
<td>Management Experience/Expertise</td>
</tr>
<tr>
<td></td>
<td>Etc.</td>
</tr>
</tbody>
</table>
Accounting Systems for SMEs

♦ QuickBooks

♦ Microsoft Dynamics (GP, SL, etc.)

♦ MAS90 (SAGE 100)

♦ Accounting spreadsheets (e.g., Excel)

♦ Cloud applications/SaaS (Software as a Service) - e.g., (e.g., NetSuite Online, QuickBooks, etc.)
IT Infrastructure for SMEs

- Internally managed server room instead of a full scale data center

- Cloud service provider (CSP) - e.g., IaaS (Infrastructure as a Service)

- Colocation Center – provides facility to house client managed IT equipment (e.g., servers, etc.)
Accounting Spreadsheets

“poorly controlled spreadsheets could result in accounting misstatements”

Risk Areas

- Formula accuracy
- Data integrity (e.g. lack of data entry controls)
- File version control
- Change management
- Fraud
- Unauthorized access
- Lack of Audit trail
- Backup & retention
- Manual intensive (increased possibility of human error)
Accounting Spreadsheets

Operational/Maintenance Controls

♦ Periodic second level (person) review of complex spreadsheet logic and formulas
♦ Backup of critical spreadsheets that support financial reporting
♦ Review of hardcoded values (e.g., tax rates)
♦ Password protection
♦ Directory access security
♦ Protection of sensitive formulas (cell protection control/cell locking)
♦ Naming convention consistency (for file identification and version control)
Accounting Spreadsheets

Security Controls

- Password protection
- Directory access security
- Protection of sensitive formulas (cell lock protection)
Accounting Spreadsheets (Continued)

**Development/Change Management Controls**
*(Maintenance Controls)*

- Document approvals for changes to spreadsheet accounting functionality (i.e., formulas, calculations, etc.)
- Testing of formulas
- Documentation of logic and business objectives

“The presence of a spreadsheet application in an accounting system can subvert all the controls in all the other parts of the systems”  ISACA Journal
Cloud Services

Delivery of computing as a service rather than a product. Provides easy and scalable access to computing resources and IT services. Software and/or hardware are housed offsite in service provider hosted facilities:

- **Software-as-a-Service (SaaS)**
- **Infrastructure-as-a-Service (IaaS)**
Cloud Services (Continued)

♦ **Software-as-a-Service (SaaS)** – Client uses applications that run on a SaaS provider’s servers. Sometimes referred to as web-based software, on-demand software (e.g., NetSuite) or hosted software. The provider manages access to the application, including security, availability, and performance.

♦ **Infrastructure-as-a-Service (IaaS)**: Client contracts with service provider for infrastructure services e.g., network, data storage, connectivity, etc.. The service provider owns the equipment and is responsible for housing, running and maintaining it.
SSAE 16 SOC 1 Type 2

- SSAE 16 - Statement for Standards for Attestation Engagements No 16
  - SOC 1 - Service Organization Control No 1; review of internal controls that are likely to be relevant to an audit of a customer’s financial statements.
  - Type 2 - reports on whether controls were suitably designed and operate effectively over a period of time, i.e., tests of controls.

**Interpretation:**

- Report Opinion: Unqualified, Qualified, Adverse
- User/Client Control Considerations Implementation
- Determine Control Risk: Low, Medium, High
Other Independent Reports

(These do not substitute for a SSAE 16 SOC1 Type2)

♦ Network Vulnerability Assessment (Third Party)

♦ SSAE 16 SOC1 Type 1 – excludes test of controls operating effectiveness

Issued under AT (Attestation Standard) Section 101:

♦ SOC2 (Type 1 & 2) - "Reports on Controls at a Service Organization over Security, Availability, Processing Integrity, Confidentiality, or Privacy".
SOC2 Principles

- **Security**: The system is protected, both logically and physically, against unauthorized access.

- **Availability**: The system is available for operation and use as committed or agreed to.

- **Processing Integrity**: System processing is complete, accurate, timely, and authorized.

- **Confidentiality**: Information that is designated “confidential” is protected as committed or agreed.

- **Privacy**: Personal information is collected, used, retained, and disclosed in conformity with the commitments in the entity’s privacy notice and with the privacy principles put forth by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).
Client’s Internal Server Room (Basic Controls)

- Physical Security (cardkey system, cipher door lock, etc.)
- Temperature Controls (Leibert system to manage temperature/humidity control, air conditioning system)
- Cabling (racks, raised floor)
- Fire Detection, Prevention and Suppression (fire extinguisher, chemical suppression system, dry pipe sprinkler system, etc.)
IT Control Areas

Application Controls

1. Data Integrity & Reporting
   - Data validation/edit checks
   - Reasonableness
   - Report access

2. Application Security
   - Password
   - File access
   - Audit Logging
   - User Roles/Profiles

IT General Computer Controls (Infrastructure)

1. Information Security
2. Change Management
3. Computer Operations
## Risk Assessment

### Control Matrix

**Audit Entity/Area:**

<table>
<thead>
<tr>
<th>No.</th>
<th>Business Risk</th>
<th>Inherent Risk Level</th>
<th>Control Objective</th>
<th>Control Activity</th>
<th>Control Activity Maturity Level</th>
<th>Residual Risk Level</th>
<th>Audit Program Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>[Risk]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Identifies **gaps in internal controls** and needed control processes.

- **Assesses the design effectiveness** of internal controls.
Process Maturity

COBIT Control Maturity Model

- **Non-existent (0)** - Complete lack of any recognizable control process
- **Initial/Ad Hoc (1)** – Control exists, but is not standardized or applied consistently
- **Repeatable but intuitive (2)** – Control is known, but is not documented, defined and communicated effectively to staff.
- **Defined Process (3)** - Control has been standardized and documented, but not managed and monitored for compliance
- **Managed and Measurable (4)** – Control is effectively managed and monitored, but efficiency may not be optimized through effective use of automation.
- **Optimized (5)** – Control is sufficiently refined to a level of best practice and is automated to ensure efficiency, as needed.
Compensating Controls for SME

- Detection controls
- Monitoring
- User security management
- Outsource transaction processing (e.g., TPA)
Compensating Controls for SME

**Detection Controls**
- Logging of transaction activity to include dates, times, changes to data, user.
- Intrusion Detection Systems

**Monitoring**
- Review of security logs, audit trails and reports to determine if inappropriate or unauthorized activity has occurred.
- Management review of access rights to ensure granted access is appropriate.

**User Security Management**
- Defined security roles that align with job functions
- Password configuration controls
- Security administration

**Outsource Transaction Processing**
(reply on control environment of third-party providers)
- Payroll processing
- Human Resources recordkeeping
CAATS – Computer Audit Assist Techniques

Definition: The use of certain software (e.g., commercially well-established products) that can be used by the auditor to perform audits and to achieve the goals of auditing.

Types of CAATS (TOOLS):

- **Data analysis software** - extracts data from accounting files and database tables to perform data analysis to include re-performance of calculations, queries for outliers/anomalies, stratification, sampling, statistical analysis, etc. (e.g., ACL, IDEA, etc.)

- **Network security evaluation software (utilities)** - review hardware and software components (e.g., firewalls, Internet routers, etc.) supporting the technical infrastructure of an organization to identify network security exposures and vulnerabilities, for example, network vulnerability scanners.
CAATS – Computer Audit Assist Techniques (Continued)

♦ Operating system and DBMS security evaluation software (utilities) – tools evaluate OS and DBMS security parameters, event logging, access privileges/permissions, services that are open/running (their associated exposures and need if any for existing), etc.

♦ Application software and code testing tools – scans software for security vulnerabilities, malicious code, flawed functionality, etc.
CAATS – Computer Audit Assist Techniques

Why?

♦ 100 percent scrutiny of large transaction files
♦ Target/zero in on erroneous/suspicious transactions
♦ Enhance audit speed and efficiency
♦ Programs are reusable
♦ Cost Recovery (identifies DUPLICAT PAYMENTS)
♦ Revenue Enhancement (identifies unbilled or unpaid A/R)

Streamlines fieldwork, reduces audit hours and can even increase profit
Key Business Cycles for Audits *

- Revenue
- Expenditures
- Inventory
- Payroll

*Material account balances typically audited for these areas
CAATS Can Assist with Auditing Financial Statement Account Balance Assertions

- **Existence or occurrence**— Assets, liabilities, and ownership interests exist at the balance sheet date as presented in the financial statements.

- **Completeness**—All transactions and other events and circumstances that occurred during a specific period have been recorded.

- **Accuracy (valuation)**—Asset, liability, revenue, and expense components are recorded at appropriate amounts.

- **Classification**—Items in the statements have been properly described, sorted, and classified.

- **Cut off**—Transactions and events have been recorded in the correct accounting period.
In Review: Areas of Focus for IT Audits of a SME

♦ Type of accounting system software used (e.g., NetSuite, QuickBooks, etc.)

♦ Spreadsheet security and control

♦ Integration of Cloud technology

♦ Compensating Controls

♦ CAATS
Q & A