

## The Role of the Information Security Assessment in a SAS 99 Audit

Stan Stahl, Ph.D.  
President  
Citadel Information Group, Inc.

*The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud.*<sup>1</sup>

### Summary

1. Vulnerabilities in the use of information technology resources expose a business to error and fraud
2. The auditor cannot obtain reasonable assurance without an information security risk and vulnerability assessment
3. Citadel's 3-pronged information security risk and vulnerability assessment fully supports the objectives of SAS 99
4. Citadel's information security risk and vulnerability assessment process integrates with SAS 99 directives on conducting the audit

### Detailed Exposition

#### ***1. Vulnerabilities in the use of information technology resources expose a business to fraud.***

*Scenario 1:* An honest but untrained human resources clerk shares her computer password with an unscrupulous coworker. The coworker logs in as the human resources clerk and gives herself a raise.

*Scenario 2:* A resident in an apartment complex takes advantage of a *Windows* bug to hack into the property management company's computers and lower his rent.

---

<sup>1</sup> Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit*, Paragraph 1, quoted from Statement on Auditing Standards (SAS) No. 1, *Codification of Auditing Standards and Procedures*, (AICPA, Professional Standards, Vol 1, AU sec.110.02, "Responsibilities and Functions of the Independent Auditor")

- Scenario 3:* A dishonest supplier takes advantage of a misconfigured firewall to change the price on an electronic invoice. The supplier changes supporting documentation to keep the books balanced.
- Scenario 4:* An unethical customer takes advantage of a security vulnerability to change his preferred pricing plan.
- Scenario 5:* The VP of operations and a junior IT person collude to use company resources to run a separate business.
- Scenario 6:* An IT administrator with extensive computing skills but little ethical understanding improperly accesses the company's general ledger at the "data file level,"<sup>2</sup> directing checks to a friend's bank account. The IT administrator also enters invoices into the computer system to keep the books balanced.
- Scenario 7:* Tony Soprano hires a hacker who takes advantage of a vulnerability in a printer to gain access to the company's information systems. The hacker inserts electronic "proofs of delivery" and invoices for disposables (light bulbs, toilet paper, etc.) which the A/P program pays as legitimate.

## ***2. The auditor cannot obtain" reasonable assurance" without an information security risk and vulnerability assessment.***

### ***Information Security Management Practices***

Information security vulnerabilities that may impact financial statement correctness exist in both the human and technical domains. Countering these vulnerabilities are ten *Information Security Management Practices*.<sup>3</sup> A business' financial information is secure only to the extent that these 10 practices are being *systematically* managed. Weaknesses in any single management practice can often negate the combined strength of the other nine.

The 10 *Information Security Management Practices* are:

1. Security Policy
2. Organizational Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Systems Development and Maintenance
9. Business Continuity Management

---

<sup>2</sup> By the "data file level" we mean the level of basic operating system read and write commands, bypassing the controls of the company's accounting system.

<sup>3</sup> These ten *Information Security Management Practices* identified in *Information Technology—Code of Practice for Information Security Management*, International Standards Organization, ISO-17799, 2000

## 10. Compliance

### ***Relationship of Ten Information Security Management Practices with SAS 99***

#### **SAS 99. Introduction and Overview**

*Management is responsible for ... establishing and maintaining internal control*<sup>4</sup>

Given the scenarios described above, management's responsibility for establishing and maintaining internal control necessarily extends to the responsibility of management for establishing and maintaining suitable *information security* controls.

#### **SAS 99. Description and Characteristics of Fraud**

*The auditor's interest specifically relates to acts that result in a material misstatement of the financial statements<sup>5</sup>, whether arising from fraudulent financial reporting or misappropriation of assets<sup>6</sup>*

As the scenarios illustrate, specific acts of misuse of computer and information systems may result in a material misstatement of the financial statements. Opportunities exist both to commit fraud and to misappropriate assets. Consequently, the auditor's interest relates to weaknesses in information security management practices that could allow, fail to prevent, or fail to audit the occurrence of improper *acts* that could result in a material misstatement.

*Three conditions generally are present when fraud occurs. ... circumstances exist—for example, the absence of controls, ineffective controls, or the ability of management to override controls—that provide an opportunity for a fraud to be perpetrated*<sup>7</sup>

Weak or ineffective information security controls, in any of the ten management practices, provide opportunity for fraud to be perpetrated.

*Management has a unique ability to perpetrate fraud ...*<sup>8</sup>

Any opportunity for management to circumvent system access and other controls provide it with the opportunity to commit fraud and to cover up the tracks of any fraud.

*Management and employees engaged in fraud will take steps to conceal the fraud<sup>9</sup> ... Fraud may also be concealed through collusion among management, employees, or third parties<sup>10</sup>*

---

<sup>4</sup> SAS 99, Paragraph 4, from SAS 1, AU sec 110.03

<sup>5</sup> SAS 99, paragraph 5

<sup>6</sup> SAS 99, paragraph 6

<sup>7</sup> SAS 99, paragraph 7

<sup>8</sup> SAS 99, paragraph 8

The absence of system auditing, or the opportunity to change audit logs, provides management, employees, and third parties with an opportunity to conceal the fraud.

Collusion between management and IT personnel, or between 3<sup>rd</sup>-parties and IT personnel, provides significant opportunity to conceal fraud.

*The presence of certain conditions may suggest to the auditor the possibility fraud may exist*<sup>11</sup>

The following is a short list of conditions, any one of which suggests the possibility that fraud may exist:

1. Unpatched system vulnerabilities, extraneous system services, or open firewall ports provide access to cyber criminals to misappropriate financial resources
2. Weak security architectures may make it too easy to improperly access the accounting servers and other network components on which financial statements depend
3. The presence of an unsecured wireless network increases the likelihood that an outsider can gain access to critical system resources and use these to misappropriate financial resources
4. A failure to control user activity on the internet increases the likelihood that an employee will download a Trojan Horse, giving control of his computer to an outsider who can misappropriate financial resources
5. User accounts that don't link to a specific appropriate person provide opportunities for system misuse by management, IT personnel, other personnel, and third parties
6. Gaps in audit logs may be the result of an attempt to conceal system misuse
7. Unauthorized forwarding of email may be indicative of serious system abuse, including fraud
8. The absence of information security policies may allow 'cracks' in the system that can be used for the commission of fraud
9. The absence of employee training and education make employees vulnerable to social engineering attacks, from management, coworkers or outsiders, that can be used to perpetrate fraud
10. Poor password management practices increase the ease with which those wishing to commit fraud can access system resources and also make fraud easier to cover up

*The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by fraud or error*<sup>12</sup>

---

<sup>9</sup> SAS 99, paragraph 9

<sup>10</sup> SAS 99, paragraph 10

<sup>11</sup> SAS 99, paragraph 11

<sup>12</sup> SAS 99, paragraph 12

As the scenarios and the above points illustrate, specific acts of misuse of computer and information systems may result in a material misstatement of the financial statements. This imposes the responsibility on the auditor to include an assessment of the ten information security management practices in planning and performing the audit.

### **SAS 99. The Importance of Exercising Professional Skepticism**

*Due professional care requires the auditor to exercise professional skepticism ... Professional skepticism is an attitude that includes a questioning mind and a critical assessment of audit evidence. The auditor should conduct the engagement with a mindset that recognizes the possibility that a material misstatement due to fraud could be present ... [P]rofessional skepticism requires an ongoing questioning of whether the information and evidence obtained suggests that a material misstatement due to fraud has occurred. In exercising professional skepticism in gathering and evaluating evidence, the auditor should not be satisfied with less-than-persuasive evidence ...<sup>13</sup>*

The above scenarios coupled with several years of statistics showing an exponential rise in both computer crime and computer vulnerabilities, establish beyond doubt that non-existent, weak or ineffective information security management practices provide extensive opportunity for acts of fraud. Consequently it follows from the SAS 99 requirement for professional skepticism that the auditor be satisfied with nothing less than persuasive evidence that management is effectively managing the ten information security management practices. Indeed, if the auditor is to conduct the engagement with a mindset that recognizes the possibility that a material misstatement due to fraud could be present, then it follows that the auditor has a responsibility to gain positive assurance about management's information security practices. Consider, as a simple example, the fact that, given the scope of computer crime, if audit logs aren't kept, the obligation for professional skepticism constrains the auditor's ability to deny the possibility that fraud may exist.

### **3. Citadel's information security risk and vulnerability assessment fully supports SAS 99.**

*Our 3-pronged information security risk and vulnerability assessment is designed to uncover weaknesses in the ten Information Security Management Practices that impact the extent to which one can have "reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud."*

*Task 1.....Information Security Management Assessment*

1. Information Security Organizational Management
2. Information Security Policies
3. Organization Culture, Employee Attitudes & Practices
4. Managing Trust in Employees

---

<sup>13</sup> SAS 99, paragraph 13

5. Information Security Awareness & Continuing Education
6. Independent 3rd-Party Review and Assessment

*Task 2.....Security Assessment of the IT Infrastructure*

1. External Network Vulnerability Scan
2. Internal Network Vulnerability Scan
3. System User Account Inventory
4. System Email Account Audit
5. Authentication Controls Effectiveness
6. Backup Security
7. IT Auditing & Monitoring

*Task 3.....IT Security Management Practices*

1. System Security Design
2. Access Control Management
3. System Security Maintenance
4. Application Security
5. System Security Audit and Review
6. Incident Response Management
7. Information Continuity Management
8. Information Security Continuing Education

**4. Citadel's assessment process integrates with SAS 99 directives on conducting the audit.**

- Discussion with engagement personnel regarding the risks of material misstatement due to fraud <sup>14</sup>
- Obtaining the information needed to identify the risks of material misstatement due to fraud <sup>15</sup>
- Identifying risks that may result in a material misstatement due to fraud <sup>16</sup>
- Assessing the identified risks after taking into account an evaluation of the entity's programs and controls that address the risks <sup>17</sup>
- Responding to the results of the assessment <sup>18</sup>

---

<sup>14</sup> SAS 99, paragraphs 14 - 18

<sup>15</sup> SAS 99, paragraphs 19 - 34

<sup>16</sup> SAS 99, paragraphs 35 - 42

<sup>17</sup> SAS 99, paragraphs 43 - 45

- Evaluating Audit Evidence <sup>19</sup>
- Communicating about possible fraud to management, the audit committee, and others <sup>20</sup>
- Documenting the auditor's consideration of fraud <sup>21</sup>

**Citadel Information Group ... Securing the critical information assets of middle market businesses, mid-sized government agencies, and the not-for-profit community.**

© Copyright 2004. Citadel Information Group, Inc. All Rights Reserved.

---

<sup>18</sup> SAS 99, paragraphs 46 - 67

<sup>19</sup> SAS 99, paragraphs 68 - 78

<sup>20</sup> SAS 99, paragraphs 79 - 82

<sup>21</sup> SAS 99, paragraphs 83