

# The Influence Of Management Tone On Security Control Strength

Tim Kizirian (Email: tkizirian@csuchico.edu), California State University, Chico

## Abstract

*This study uses archival information technology (IT) audit documentation from 60 auditees of a Big 4 firm to examine whether management's security tone and activities affect security controls. The IT auditor's assessment of the reliability of security controls surrounding a client's information system is a vital component of the audit process. Findings in this study indicate a positive relationship between the strength of management tone surrounding information system security and the IT auditor's assessment of security controls strength. The findings indicate the utilization of management security tone assessments during an IT audit, and thus, provide objective evidence on the importance of an organization's tone at the top.*

## 1. Introduction

Financial statement auditors utilize the special skills of IT auditors to understand and assess the reliability of controls that address system related risks. Using evidence from a Big 4 firm's IT audit workpapers, I hypothesize and find that the IT auditor's assessment of management tone surrounding system security (management security tone) influences the assessed strength of security controls. This finding holds even after consideration of management activities that also promote a strong security control environment, confirming the overriding importance of management security tone for strong security controls. Despite its importance, I am unaware of any empirical research examining the management security tone – security control strength relationship. Prior research has been unable to test this relation using archival data possibly due to the limited nature of audit evidence.

This study utilizes three measures of management activity that significantly relate to the IT auditor's security control strength assessment: the IT auditor's management security tone assessment, the presence/absence of an independent information security governance function, and the presence/absence of effective communication of information security policies and procedures to employees. The IT auditor's management security tone assessment attempts to capture the *attitude* of management regarding security control. While it is essential for IT auditors to understand the control policies and activities management has put into place, an understanding of management's attitude toward controls is of paramount importance. Results indicate that this assessment of attitude is a tremendous driver of the IT auditor's security control assessment, subsuming the effect of an independent governance function and communication of policies and procedures, suggesting an "attitude over activities" assessment behavior.

Results support authoritative guidance suggesting that management involvement in setting the security tone of the organization should drive the security control environment and promote effective placement and operation of security controls (e.g., SAS 94; COBIT 2002). Prior literature has identified that management tone at the top is a key factor for reliable financial reporting and sound internal control (e.g., D'Aquila 1998; Wong-on-Wing, Reneau and West 1989).<sup>1</sup>

---

<sup>1</sup> The Treadway Commission (1987) identifies the tone at the top as the most important contributing factor to the integrity of information.

Management's level of control consciousness is a key determinant of the client's risk structure and is at the foundation of internal control. Without a strong "tone at the top," it is unlikely even the most proficient internal controls will be effective in preventing, detecting and correcting errors and irregularities. Even the best security policies and procedures are susceptible to management collusion and override. Hence, it is useful to evaluate evidence on whether auditors incorporate this important risk component into their audit judgments. This field-based workpaper evidence containing auditor assessments provides objective judgments of management security tone and security control strength.

The paper proceeds as follows. Section two outlines the hypotheses. Section three describes the data and the empirical tests. Section four provides results and section five summarizes findings.

## **2. Literature Review And Hypothesis Development**

### **2.1. The Audit Process**

Financial statement auditing standards guide auditors to base their effort allocation on explicit risk assessments concerning material misstatements in the financial statements (The Audit Risk Model, SAS 47). The second Generally Accepted Auditing Standard of fieldwork states that a sufficient understanding of internal control is required to plan the audit and to determine the nature, timing and extent of tests to be performed (e.g., SAS 47, 78, 94).<sup>2</sup> In obtaining a "sufficient understanding," the auditor should consider how an entity's use of information technology may affect controls relevant to management's assertions (SAS 94). Financial statement auditors conventionally use IT specialists to assess the reliability of systems and security controls.

Current business practices necessitate the utilization of information technology to efficiently handle complex transactions. Where a significant amount of financial statement information is electronically initiated, recorded, processed, or reported, it may not be possible to design effective substantive audit tests without assessing computer systems and security controls (SAS 79, 94; Greene 2002; Guldentops 2001). For some firms, systems and security controls may be more relevant than non-systems controls for the prevention, detection and correction of material misstatements (Bagranoff and Vendrzyk 2000; Tucker 2001).

Advances in information technology often require controls specific to the computer system (Anderson 1976). System controls serve to ensure completeness, accuracy and validity of financial information produced by the computer system. Improvements in systems technology, programs, and procedures could improve the control environment and subsequently reduce the auditor's control risk assessment (ISACA 2002; SAS 47, 78, 94).<sup>3</sup> Due to the widespread reliance on information systems, the Committee of Sponsoring Organizations Framework provides specific controls guidance for computer related activities (COSO 1999; AICPA 2000).

### **2.2. Security Controls**

Effective security controls provide reasonable assurance that continually changing business processes and technology do not introduce security risks. Well-designed security controls may reduce errors and irregularities by means of effective prevention, detection and correction (Guldentops 2001). Successful operation of most internal controls is dependent on security controls being in place and operating effectively (ISACA 2002). Ineffective security controls leave open the opportunity for unauthorized access to application programs and databases. The prevention of unauthorized physical and logical access to software and related data files are conventional security control goals. Typical physical security controls restrict access to hardware, software and datasets by means of locked doors, badge entry systems, and security personnel. Logical access controls restrict user access to specific,

---

<sup>2</sup> The Sarbanes-Oxley Act also requires that auditors of publicly held clients evaluate information system effectiveness.

<sup>3</sup> Through the linkage promoted in the Audit Risk Model (SAS 47), a lower control risk assessment should lead to less total audit effort (e.g., Pany and Whittington 2001).

authorized data, and then only to perform specific functions. Restriction is typically accomplished by means of user ID's and passwords, physical possession and biometric identification.

### **2.3. Management's Influence on Security Controls**

Authoritative guidance and prior literature agree on the importance of management tone in setting internal control standards. In an experiment using 60 auditors from national accounting firms, Kaplan and Reckers (1984) find that management control consciousness affects preliminary judgments of the effectiveness of internal controls. In an experiment using 117 auditors from a large international public accounting firm, Wong-on-Wing, Reneau and West (1989) point out that the auditor's assessment of management tone toward internal control influences key audit judgments such as the nature, timing and extent of audit testing. D'Aquila 1998 obtained survey evidence from 196 CPA's providing evidence to support the notion that management's attitude toward internal control is a significant consideration in the evaluation of a firm's control environment.

The Committee of Sponsoring Organizations (COSO) frames the tone at the top as arguably the most important component of a control structure (COSO 1999). Without management's dedication to the security control structure it is unlikely that even the most state of the art security controls will be effective in detecting and preventing violations that may lead to financial statement misstatements. COSO 1999 states:

*The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.*

Management involvement in setting the security tone for the organization includes the approval and support of information security policies and procedures, and resource commitment (ISACA 2002). Management's security policies include adopting a mission statement and agreed upon goals and objectives for security control activities. Management with a strong control consciousness will typically employ an independent information security governance function and will effectively communicate information security policies and procedures to all employees in order to promote the effective and efficient operation of security control procedures (COBIT 2002). Established control procedures work to provide a strong control environment and provide reasonable assurance that the entities' security objectives will be achieved. SAS 94 states:

*Management's failure to commit sufficient resources to address security risks presented by information technology may adversely affect internal control by allowing improper changes to be made to computer programs or to data, or by allowing unauthorized transactions to be processed.*

As indicated in authoritative guidance (COBIT 2002; ISACA 2002), management security tone should provide the basis for developing security control policies and procedures that are in place and operating effectively. IT auditor's test the detailed technical procedures relating to the manner in which to secure specific applications, operating systems, or other IT components. It is possible that management security tone positively affects the strength of these detailed security control procedures leading to Hypothesis One:

**H1:** The IT auditor's assessment of management security tone will directly affect the IT auditor's assessment of security control strength.

Management activities such as the employment of an independent information security governance function and the communication of information security policies and procedures also promote the effective and efficient operation of security control procedures. Professional guidance encourages the establishment of an independent security function to implement management's goals and objectives, and considers the function to be a distinguishing component of an effective security controls framework (e.g., ISACA 2002, SAS 94, COBIT 2002).

Professional guidance also encourages effective communication of security policies and procedures to all employees as this contributes to a strong security control structure. The IT auditor should assess whether security policies and procedures are consistently communicated, either orally or in writing. Professional guidance promotes

signed information security awareness agreements by all end-users. Unwritten policies should be well understood and consistently implemented in practice. This leads to Hypothesis Two and Three:

**H2:** Management's employment of an independent security governance function will directly affect the IT auditor's assessment of security control strength.

**H3:** Management's communication of security policies and procedures to all employees will directly affect the IT auditor's assessment of security control strength.

The employment of a security governance function, and communication of security policies and procedures are easily determinable and may independently affect security control strength. The IT auditor's management security tone assessment is more judgmental in nature and potentially more difficult to quantify as it attempts to capture the attitude of management regarding security control. Regardless of potential assessment difficulties, extant research and professional guidance (e.g., SAS 94; Wong-on-Wing, Reneau and West 1989) strongly promote management security tone as the key driver of the effective placement and operation of controls, leading to Hypothesis Four:

**H4:** The IT auditor's assessment of management security tone will directly affect the IT auditor's assessment of security control strength, subsuming the effect of management's employment of an independent security governance function and management's communication of security policies and procedures.

### 3. Proprietary Data, Variable Measurement And Model Specification

#### 3.1. Proprietary Data

The IT audit documentation used in this study is acquired from a Big 4 firm that utilizes the expertise of in-house IT auditors to assess systems and security controls of its clients. The firm granted access to its archived audit working paper records for a given practice office having a mostly technology client base. Using a random number generator, sample audits were selected from the list of archived engagements containing audit files from 1996 to 1999. The accounting firm provided data for 60 engagements, representing 60 different firms. The Big 4 firm has been auditing these clients for an average of seven years, and 54 of the auditees are publicly traded companies. The auditing firm assisted in the coding of variables used in this study, and provided a subsequent review to facilitate consistency of coding. Each of the 60 firm-year IT audit observations include the auditor's documented assessment of the overall strength of security controls, an assessment of the strength of management security tone, whether management employs an independent information security governance function, and whether management communicates information security policies and procedures to employees.

#### 3.2. Variable Measurement And Model Specification

To test H1, a multiple OLS regression is employed in the following form:

$$SEC_i = \beta_{0i} + \beta_1 MST_i + \beta_2 TA_i + \beta_3 YA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i \quad (1)$$

The dependent variable is the IT auditor's firm-wide assessment of security control strength (SEC), documented as "strong," "moderate," or "weak." This assessment is coded 3 for strong, 2 for moderate, and 1 for weak. SEC is a summary metric that takes into consideration the strength of the security control environment, systems, policies and control procedures taken as a whole. The assessment is conducted in a manner consistent with generally accepted standards (e.g., SAS 94, ISACA 2002).

The test variable is the IT auditor's assessment of management security tone (MST). The IT auditors in our study arrive at the assessment by investigating factors relating to management's *attitude* toward security control consciousness (e.g., the importance placed on security controls). Due to the largely unobservable and subjective nature of MST, the audit firm provides limited guidance on specific factors to be considered in the assessment.

However, the assurances firm guides the IT auditor to make the assessment in a holistic manner based primarily on inquiry of management about the placement and operation of security procedures, as well as evidence from an adequate understanding of the client's security control structure and any relevant security control evidence from other parts of the IT or financial statement audit. MST is documented similar to SEC and is also coded 3 for strong, 2 for moderate, and 1 for a weak MST assessment. With SEC as the dependent variable, the coefficient on MST is expected to obtain a positive value, indicating that strong management security tone will be associated with strong security controls.

Included are several variables to control for potential influences on SEC. Prior literature has noted that the length of the auditor-auditee relationship may affect auditor assessments due to learning over time (O'Keefe, Simunic and Stein 1994; Ashton 1991). Including the number of years the auditor has been auditing the auditee (YA) controls for this potential affect. As a result of the audit process, the auditee should attain an understanding of control deficiencies to be mitigated. Over time these refinements should result in an improvement in the strength of security controls, resulting in a positive coefficient on YA.

To control for auditee size, I include the natural log of the book value of total auditee assets (TA) for the year under audit. Prior literature has shown that the relationship between auditor assessments and client size is nonlinear (O'Keefe et al 1994). To address this issue, the natural log of total assets is utilized. While larger firms may have more resources leading to potentially stronger security controls, they may have more complex control structures and greater decentralization, potentially increasing security risks. It is unclear how these effects will aggregate and affect the relationship between assessed strength of security controls and management security tone. Accordingly, there is no expectation of the sign on TA.

Prior research suggests the auditor is more likely to be sued if the auditee is publicly held (e.g., St. Pierre and Anderson 1982). Additionally, incentives to override controls to overstate financial standing and results of operations are suggested to be greater for managers of public firms due to market driven compensation structures (O'Keefe et al 1994). In order to compensate for the related increase in auditor business risk, public client's system controls are likely to bear greater scrutiny. This is controlled for by including an indicator variable for public firms (PUB) which is expected to exhibit a positive association with SEC.

To control for potential systematic differences in the manner in which IT audits are conducted between industry groups as identified by the data-granting firm, IND is included. IND is an indicator variable representing the two industry subcategories in our sample. Given the lack of evidence concerning major changes in audit approach by the data-granting firm between industry groups, no expectation is held for the coefficient on IND.

To test H2, a multiple OLS regression is employed in the following form:

$$SEC_i = \beta_{0i} + \beta_1FUNCTION_i + \beta_2TA_i + \beta_3YA_i + \beta_4PUB_i + \beta_5IND_i + e_i \quad (2)$$

The test variable FUNCTION equals one if management employs an independent information security governance function, and zero otherwise. With FUNCTION as an independent variable, the coefficient on SEC is expected to obtain a positive value, indicating that security control strength will be positively affected by the presence of an independent security function.

To test H3, a multiple OLS regression is employed in the following form:

$$SEC_i = \beta_{0i} + \beta_1COMM_i + \beta_2TA_i + \beta_3YA_i + \beta_4PUB_i + \beta_5IND_i + e_i \quad (3)$$

The test variable COMM equals one if the IT auditor assesses that management communicates information security policies and procedures to all employees, and zero otherwise. With COMM as an independent variable, the coefficient on SEC is expected to obtain a positive value, indicating that security control strength will be positively affected by the presence of communication of information security policies and procedures.

To test H4, a multiple OLS regression is employed in the following form:

$$SEC_i = \beta_{0i} + \beta_1MST_i + \beta_2FUNCTION_i + \beta_3COMM_i + \beta_4TA_i + \beta_5YA_i + \beta_6PUB_i + \beta_7IND_i + e_i \quad (4)$$

The coefficient on MST is expected to obtain a positive value, indicating that strong management security tone will positively affect the security control strength assessment. Given the strong promotion of MST as the key driver of security control strength in the extant literature and professional guidance, FUNCTION and COMM are expected to obtain insignificant coefficients.

#### 4. Results

Table 1 presents OLS regression results for Equations 1-3, which utilize SEC as a dependent variable and MST, FUNCTION and COMM, respectively, as test variables. Equations 1-3 obtain significant, positive coefficients on MST (0.7621,  $p < 0.0001$ ), FUNCTION (0.6748,  $p < 0.0001$ ) and COMM (0.7295,  $p < 0.0001$ ), respectively, providing evidence to support H1-H3. These results indicate that management security tone, the presence of an information security governance function, and communication of information security policies and procedures positively affect the IT auditor's judgment of security controls strength when considered independently. Equation 1-3 variance inflation factors (VIFs) do not exceed 1.78 indicating multicollinearity does not affect these results.<sup>4</sup> The larger R-squared value for Equation 1 using MST as a test variable (76.15%) implies that MST affects SEC to a greater degree than do FUNCTION (43.38%) and COMM (52.95%).

Table 2 presents OLS regression results for Equation 4, which utilizes SEC as a dependent variable and includes MST, FUNCTION and COMM as independent variables in a single regression model. MST obtains a significant, positive coefficient (0.7424,  $p < 0.0001$ ), while FUNCTION (-0.0061,  $p = 0.9627$ ) and COMM (0.0385,  $p = 0.7727$ ) do not obtain significant coefficients.<sup>5</sup> This result indicates that management security tone positively affect the IT auditor's judgment of security controls strength and subsumes the effect of the presence of an information security governance function and communication of information security policies and procedures to all employees. When taken in conjunction with the superior Table 1 R-squared values using MST, these findings support the notion that management security tone is a key driver of the effective placement and operation of security controls (e.g., Wong-on-Wing, Reneau and West 1989).

#### 5. Summary And Conclusions

This study examines factors influencing the IT auditor's assessment of the strength of security controls using objective IT auditor workpaper evidence. Incorporated in the examination are measures of management attitude (the security tone assessment) and management activities (employment of an independent information security governance function and communication of information security policies and procedures). When examined independently, these measures are directly associated with the IT auditor's assessed strength of security controls. When considered together, the management security tone assessment subsumes the influence of the management activities.

The dominant affect of the management security tone assessment is consistent with professional guidance and prior literature on the importance of management tone. While this finding may not be unexpected, it does indicate that the management security tone assessment represents a viable IT auditor consideration. The findings corroborate the importance of learning about an organization's tone at the top during an audit (D'Aquila 1998). IT managers should understand the importance of management tone, and that funding and support of a healthy tone at the top is likely to be effective in enhancing control and significantly contributes to the overall security of systems.


The data is drawn from one specific office of one Big 4 firm, potentially reducing the generalizability of results. However, the single data source also reduces the variability in controls assessments due to the homogeneity of auditor training and the application of a consistent level of acceptable audit risk.

<sup>4</sup> Marquandt (1980) argues that a multicollinearity problem exists if VIF values exceed 10.

<sup>5</sup> VIF's do not exceed 4.69 in Equation 4.

## 6. Suggestions For Future Research

The results of this study have implications to IT auditing practice and to future research. First, it is possible that IT auditors may be more efficient to collapse several time-consuming assessments into one management tone assessment, moving toward a “most important assessment.” Given the strong explanatory power of the management security tone assessment, it may potentially overlap several security control assessment factors and may efficiently and effectively subsume the variability of those factors. Future research could provide more detailed evidence as to which control factors tend to be subsumed by the management tone assessment. Second, results seem to suggest that an assessment of management attitude holds greater importance than management activities, suggesting a potential “attitude over activities” assessment behavior. Future research could investigate the weighting of management tone and management activity assessments to provide further insight on auditor assessment behavior.

While judgment and measurement issues are not the focus of this study, findings also suggest that IT auditor’s are not limited to utilizing straightforward, quantifiable measures (e.g., management activities), but also respond to judgmental, qualitative assessments derived from inquiry of management and employees (e.g., the security tone of management). Future research may consider capturing judgmental assessments similar to the data-granting firm’s management tone metric, as such assessments appear to be key considerations in the IT audit decision process. 

---

*I thank the data-granting firm for their provision of data, and gratefully acknowledge the University of Arizona Department of Accounting, and Craig and Joan Young whose generous support enabled this study. Comments by Thomas Calderon, Ronny Daigle, Bill Felix, Audrey Gramling, Wallace Lease and Dwight Sneathen were especially useful.*

## References

1. American Institute of Certified Public Accountants (AICPA). 2000. *The Panel on Audit Effectiveness Report and Recommendations to the Auditing Standards Board*. May 2000.
2. \_\_\_\_\_. 1983. “Audit Risk and Materiality in Conducting an Audit”, *Statement on Auditing Standards No. 47*. New York, NY: AICPA.
3. \_\_\_\_\_. 1995. “Consideration of Internal Control in a Financial Statement Audit: An Amendment to Statement on Auditing Standards No. 55”, *Statement on Auditing Standards No. 78*. New York, NY: AICPA.
4. \_\_\_\_\_. 1995. “Reports on Audited Financial Statements”. *Statement on Auditing Standards No. 79*. New York, NY: AICPA.
5. \_\_\_\_\_. 2001. “The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit”. *Statement on Auditing Standards No. 94*. New York, NY: AICPA.
6. Anderson, R. J. 1976. “Computer controls – an essential commodity in computer systems development”, *The Internal Auditor*. Altamonte Springs. April 1976.
7. Ashton, A. H. 1991. “Experience and error frequency knowledge as potential determinants of audit expertise”, *The Accounting Review* 66 (April): 218-239.
8. Bagranoff, N. A. and Valaria, P. V. 2000. “The Changing Role of IS Audit Among the Big Five US-Based Accounting Firms”, *Information Systems Control Journal*. Volume 5, 2000.
9. *Control Objectives for Information and related Technology (COBIT) 3<sup>rd</sup> Edition*. 2002. Copyright © 2002 by the Information Systems Audit and Control Foundation (ISACF).
10. COSO. 1999. Research promoted by the Committee of Sponsoring Organizations of the Treadway Commission, *Fraudulent Financial Reporting. 1987-1997. An Analysis of U.S. Public Companies*. For useful summarization of relevant COSO research see: (a) Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992), *Internal Control: Integrated Framework: Framework*, Coopers & Lybrand, September and/or (b) Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992), *Internal Control: Integrated Framework: Evaluation Tools*, Coopers & Lybrand, September.

11. D'Aquila J. M. 1988. "Is the control environment related to financial reporting decisions?" *Managerial Auditing Journal*. Volume 13, Number 8. 1998
12. Guldentops, E. 2001. "Harnessing IT for Secure, Profitable Use", *Information Systems Control Journal*, Volume 5, 2001
13. Greene, F. 2002. "A Survey of Application Security in Current International Standards". *Information Systems Control Journal*, Volume 6, 2002
14. ISACA. 2002. "Information Systems Auditing Standards, Guidelines and Procedures", *Information Systems Audit and Control Association (ISACA)*. ISACA Standards © Copyright 2002. Rolling Meadows, IL.
15. Kaplan, S.E., and P.M.J. Reckers. 1984. "An empirical examination of auditors' initial planning processes", *Auditing: A Journal of Practice & Theory* (Vol. 4 No. 1, Fall): 1-19.
16. Marquandt, D. 1980. "You should standardize the predictor variables in your regression models. Discussion of: A critique of some ridge regression methods", *Journal of the American Statistical Association*. 87-91.
17. O'Keefe, T. B., D. A. Simunic, and M. T. Stein. 1994. "The production of audit services: Evidence from a major public accounting firm", *Journal of Accounting Research* (Autumn): 241-261.
18. Pany, K.J. and O.R. Whittington. 2001. "Research implications of the Auditing Standard Board's current agenda", *Accounting Horizons*: 401-411.
19. St. Pierre, K. and J. Anderson. 1982. "An Analysis of Audit Failures Based on Documented Legal Cases", *Journal of Accounting, Auditing & Finance*. Boston. Spring 1982.
20. Treadway, J.C. Jr. 1987. "Report of the National Commission on Fraudulent Financial Reporting", *National Commission on Fraudulent Financial Reporting* (Treadway Commission), Washington, DC, October. 1987.
21. Tucker, G. 2001. "IT and the audit", *Journal of Accountancy*. American Institute of Certified Public Accountants (AICPA). September 2001.
22. Wong-on-Wing, B., J.H. Reneau and S.G. West. 1989. "Auditors' Perception of Management: Determinants and Consequences", *Accounting, Organizations and Society* (Vol. 14 No. 5/6): 577-590.



**TABLE 1**  
**OLS Regression Analysis (N=60)**

**Test of H1:**  $SEC_i = \beta_{0i} + \beta_1MST_i + \beta_2TA_i + \beta_3YA_i + \beta_4PUB_i + \beta_5IND_i + e_i$  [1]  
**Test of H2:**  $SEC_i = \beta_{0i} + \beta_1FUNCTION_i + \beta_2TA_i + \beta_3YA_i + \beta_4PUB_i + \beta_5IND_i + e_i$  [2]  
**Test of H3:**  $SEC_i = \beta_{0i} + \beta_1COMM_i + \beta_2TA_i + \beta_3YA_i + \beta_4PUB_i + \beta_5IND_i + e_i$  [3]

**Dependent Variable: Assessed Security Controls Strength (SEC)**

**Independent Variables and Expected Signs**

Intercept		0.5365 <i>0.2690</i>	0.8027 <i>0.2895</i>	0.6135 <i>0.3687</i>
Management Tone (MST)	+	0.7621*** <0.0001		
Governance (FUNCTION)	+		0.6748*** <0.0001	
Communication (COMM)	+			0.7295*** <0.0001
Total Assets (TA)	?	-0.0041 <i>0.8934</i>	0.0316 <i>0.5009</i>	0.0380 <i>0.3721</i>
Years as Auditor (YA)	+	0.0099 <i>0.4109</i>	0.0315* <i>0.0877</i>	0.0381* <i>0.0222</i>
Public/Private (PUB)	+	-0.0679 <i>0.6323</i>	0.0402 <i>0.8536</i>	-0.1479 <i>0.4652</i>
Industry (IND)	?	0.0003 <i>0.9974</i>	0.0789 <i>0.5955</i>	0.1462 <i>0.2750</i>
Adjusted R-squared		76.15%	43.38%	52.95%

The dependent variable is the IT auditor's assessed strength of security controls (SEC). The experimental variables include MST which is the IT auditor's assessed strength of management security tone, FUNCTION equals one if management employs an independent information security governance function, and zero otherwise, and COMM equals one if the IT auditor assesses that management communicates information security policies and procedures to all employees, and zero otherwise. Both SEC and MST take on values of 3, 2, or 1, where 3 represents strong levels of control/management tone. The control variables include the natural log of total assets (TA), the years as auditor (YA), an indicator variable for public or private ownership (PUB) where 1 equals public, and the auditor's industry classification (IND). Statistical significance for parameter estimates are indicated at the 1% (\*\*\*), 5% (\*\*), and 10% (\*) levels. All tests are one-tailed.

**TABLE 2**  
**OLS Regression Analysis (N=60)**

**Test of H4:**  $SEC_i = \beta_{0i} + \beta_1MST_i + \beta_2FUNCTION_i + \beta_3COMM_i + \beta_4TA_i + \beta_5YA_i + \beta_6PUB_i + \beta_7IND_i + e_i$  [4]

**Dependent Variable: Assessed Security Controls Strength (SEC)**

**Independent Variables and Expected Signs**

Intercept		0.5440	
		0.2812	
Management Tone (MST)	+	0.7424***	<0.0001
Governance (FUNCTION)	+	-0.0061	0.9627
Communication (COMM)	+	0.0385	0.7727
Total Assets (TA)	?	-0.0034	0.9128
Years as Auditor (YA)	+	0.0105	0.3982
Public/Private (PUB)	+	0.0759	0.6057
Industry (IND)	?	0.0036	0.9710
Adjusted R-squared		75.27%	

The dependent variable is the IT auditor’s assessed strength of security controls (SEC). The experimental variables include MST which is the IT auditor’s assessed strength of management security tone, FUNCTION equals one if management employs an independent information security governance function, and zero otherwise, and COMM equals one if the IT auditor assesses that management communicates information security policies and procedures to all employees, and zero otherwise. Both SEC and MST take on values of 3, 2, or 1, where 3 represents strong levels of control/management tone. The control variables include the natural log of total assets (TA), the years as auditor (YA), an indicator variable for public or private ownership (PUB) where 1 equals public, and the auditor’s industry classification (IND). Statistical significance for parameter estimates are indicated at the 1% (\*\*\*), 5% (\*\*) and 10% (\*) levels. All tests are one-tailed.