The Impact Of Management Security Control Consciousness On Security Control Activities: Implications For Compliance With The Sarbanes-Oxley Act

Tim Kizirian, (E-mail: tkizirian@csuchico.edu), California State University, Chico
Wallace Leese, (E-mail: wleese@csuchico.edu), California State University, Chico
James M. Kohlmeyer III, (E-mail: kohlmeyerj@mail.ecu.edu), East Carolina University

Abstract

Using information system audit documentation from 60 clients of a Big 4 firm, we extend Kizirian (2004) by examining whether management security control consciousness (i.e., the "tone at the top") influences (1) security control activities performed by the client, and (2) the auditor's firm-wide (i.e., global) assessment of security control. Findings suggest that management control consciousness results in the employment of security controls. The auditor's assessment of the strength of management control consciousness can also affect the auditor's assessment of the client's global security control. While our data pre-dates the Sarbanes-Oxley Act, our findings speak to the importance of assessing an organization's tone at the top, and thus, have implications for auditors working to certify a client's compliance with the Sarbanes-Oxley Act.

1. Introduction

Using evidence from a Big 4 firm's information system (IS) audit workpapers, we hypothesize and find that the IS auditor's assessment of management control consciousness surrounding system security influences (1) whether security controls are employed by management, and (2) the IS auditor's global assessment of the client's security control strength.[1] Regression analyses reveal a direct relationship between strong management security control consciousness and the employment of security controls.[2]

We examine the effect of management security control consciousness (as assessed and documented by the IS auditor) on the presence or absence of security control procedures. The security control procedures we investigate include (1) the employment of an independent information security governance function, (2) effective communication of information security policies, (3) utilization of security software, adequate (4) logical and (5) physical security controls, and (6) adequate reviews of security violations. The IS auditor's management security control consciousness assessment attempts to capture the attitude of the client's management regarding security control. Results indicate that this assessment of attitude is an important driver of key security control procedures, and thus, suggests that an understanding of management's attitude toward internal controls is of paramount importance.

[1] On this second finding, we extend Kizirian (2004) by including additional security control procedures in the analysis. The management security control consciousness variable in this paper is equivalent to the management security tone variable used in Kizirian (2004).
[2] We refine our analysis by addressing statistical complexities stemming from management's ability to mitigate risks using several security control procedures simultaneously.

Management control consciousness influences an organization's internal control structure and is at the foundation of internal control. It is for this reason that our study has implications for internal control compliance with the Sarbanes-Oxley Act of 2002. The passage of the Sarbanes-Oxley Act with its renewed emphasis on the effectiveness of internal control in the information system affirms the need for the auditor to obtain a sufficient understanding of management's attitude toward security control consciousness. Section 404 of the Sarbanes-Oxley Act emphasizes the importance of reliable system controls for preventing, detecting, and correcting material financial statement misstatements. Successful operation of most internal controls is dependent on security controls being in place and operating effectively (Guldentops 2001). While Sarbanes-Oxley doesn't mandate specific security controls, it would be inconceivable for an audit partner to sign off on the validity of internal controls if the systems that maintain them are insecure. Auditors who are concerned with their client's Sarbanes-Oxley compliance should consider a review of the existing security policies and processes to ensure that internal control systems remain stable.

Our research suggests that a portion of this security review should include an assessment of management's attitude toward security controls. Without a strong "tone at the top," even the most proficient controls may be ineffective in preventing and detecting errors and fraud. Even state-of-the-art control policies and procedures are susceptible to management collusion and override. Given the importance of strong management security control consciousness for effective internal control, it is useful to evaluate evidence on whether IS auditors incorporate this important judgment into the audit process. Our results support authoritative guidance suggesting that management involvement in setting the security control consciousness of the organization should drive the security control environment and promote effective placement and operation of security control activities (i.e., SAS 94; COBIT 2002).

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

2. Literature Review and Hypothesis Development

2.1. Security controls and the Sarbanes-Oxley Act of 2002

Section 404 is an especially critical portion of the Sarbanes-Oxley Act because it requires business process audits and documentation to support internal controls certification. Section 404 requires that organizations have controls in place to provide reasonable assurance that the accounting information system properly authorizes and records transactions, and that assets are safeguarded. The accounting information system must be designed to produce reliable financial statements. Where a significant amount of financial statement information is electronically initiated, recorded, processed, or reported, it may not be possible for IS auditors to assure the reliability of financial statements without assessing computer system and security controls (SAS 79, 94; Greene 2002; Guldentops 2001).[3]

The primary focus of the Sarbanes-Oxley Act is on data integrity, and data integrity without security controls cannot reasonably be achieved (Bakshi 2004). Sarbanes-Oxley compliance will require internal controls that are robust to security violations. To address these requirements, organizations are performing system security audits to ensure their accounting information systems comply with management's security policies and procedures and mitigate security vulnerabilities. Depending on the level of an organizations systems-dependency, system and security controls may be more relevant than non-system controls for the prevention, detection and correction of material financial statement misstatements (Bagranoff and Vendrzyk 2000; Tucker 2001).

Effective security controls provide reasonable assurance that continually changing business processes and technology do not introduce security risks (Guldentops 2001). Successful operation of most internal controls is dependent on security controls being in place and operating effectively (ISACA 2002). Ineffective security controls

[3] The Committee of Sponsoring Organizations Framework provides specific controls guidance for computer related activities (COSO 1999; AICPA 2000).

leave open the opportunity for unauthorized access to application programs and databases. Thus, security controls serve to ensure completeness, accuracy and validity of financial information produced by the accounting information system.

2.2 Management Control Consciousness and the Sarbanes-Oxley Act of 2002

One of the major emphases of the Sarbanes-Oxley Act is the promotion of accountability and a spirit of honesty of information in the organization's culture. An organization promoting such a culture should produce financial statement information that provides users with an accurate picture of the organization's financial position. Honesty and accountability, which depend on a management team with strong integrity and control consciousness, are the pillars of reliable financial reporting. While management integrity and control consciousness are difficult to legislate, they appear to be as important to the production of reliable financial statements as the actual performance of control procedures (Bakshi 2004). The Treadway Commission identifies the tone at the top as the most important contributing factor to the integrity of information (Treadway 1987).

Authoritative guidance and prior literature agree on the importance of management control consciousness in setting internal control standards (e.g., Bakshi 2004, COSO 1999). Using IS audit workpaper data, Kizirian (2004) finds that management security control consciousness directly influences the IS auditor's assessment of the global strength of security controls (the firm-wide strength of all security control procedures taken as a whole). This influence on the global strength of security controls held even after controlling for two time-honored security control activities: the employment of an independent information security governance function and the effective communication of information security policies and procedures. 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) find that the auditor's assessment of management control consciousness 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 suggest that management's attitude toward internal control is a significant consideration in the CPA's evaluation of a client's control environment.

The Committee of Sponsoring Organizations (COSO) frames management control consciousness as arguably the most important component of a control environment (COSO 1999). Without management's dedication to the security control environment it is unlikely that even the most state of the art security controls will be effective in preventing and detecting 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 environment for the organization includes the approval and support of information security policies and procedures, as well as resource commitment (ISACA 2002).[4] Managers with strong security control consciousness will typically employ an independent information security governance function and will effectively communicate information security policies and procedures to all employees to promote effective and efficient security procedures (COBIT 2002). Established control procedures such as logical and physical security controls, reviews of security violations, and the utilization of security software provide reasonable assurance that the entities' security objectives will be achieved.

As indicated in authoritative guidance (COBIT 2002; ISACA 2002), management security control consciousness should provide the basis for developing security control policies and procedures that are in place and operating effectively. IS auditors assess policies and procedures that secure specific applications, operating systems,

[4] Management's security policies include adopting a mission statement and agreed upon goals and objectives for security control activities. With respect to resource commitment, 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."

and other system components. It is possible that management security control consciousness directly affects the strength of these detailed security control policies and procedures.

2.3 Hypotheses

The employment of an independent information security governance function promotes 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). Control conscious management should exhibit a higher propensity to employ an independent security governance function, leading to Hypothesis One:

H1: Management security control consciousness will directly affect the employment of an independent security governance function.

Effective communication of security policies and procedures to all employees contributes to a positive security control environment. The IS 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. Control conscious management should exhibit a higher propensity to communicate security policies and procedures to all employees, leading to Hypothesis Two:

H2: Management security control consciousness will directly affect the communication of security policies and procedures to all employees.

The utilization of software that prevents, detects and corrects errors and irregularities, allowing only authorized access and changes to data is promoted by professional guidance (e.g., ISACA 2002, SAS 94, COBIT 2002). Control conscious management should exhibit a higher propensity to utilize security software, leading to Hypothesis Three:

H3: Management security control consciousness will directly affect the utilization of security software.

Authoritative guidance promotes the implementation and maintenance of adequate logical data access controls and physical access controls over servers and CPUs. Logical access controls restrict access to data by discriminating between authorized and unauthorized users. The controls draw on user knowledge (e.g., passwords) or possession (e.g., physical possession identification) in determining whether access to data is authorized. Physical access controls work to provide assurance that only authorized personnel have access to the appropriate computer equipment. Physical access controls include such items as placing computer equipment in locked rooms and requiring proper employee identification such as security badges. Control conscious management should exhibit a higher propensity to enforce logical and physical access controls, leading to Hypothesis Four and Five:

H4: Management security control consciousness will directly affect the implementation and maintenance of logical access controls.

H5: Management security control consciousness will directly affect the implementation and maintenance of physical access controls.

The periodic review of security violation logs and the timely resolution of related security breeches is considered to be a fundamental security control (e.g., ISACA 2002). Control conscious management should exhibit a higher propensity to review security violations, leading to Hypothesis Six:

H6: Management security control consciousness will directly affect the review of security violations.

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. Kizirian (2004) tested and found that The IS auditor's assessment of management security control consciousness directly affected the IS auditor's global assessment of security control strength. This result was found after controlling for two security control activities: management's employment of an independent security governance function and management's communication of security policies and procedures. In Hypothesis Seven, we extend Kizirian (2004) by controlling for a *comprehensive* set of security control activities which should lead to a more powerful test of the importance of management control consciousness.

H7: The IS auditor's assessment of management security control consciousness will directly affect the IS auditor's global assessment of security control strength, controlling for the effect of the following security control activities: the employment of an independent information security governance function, management's communication of information security policies, utilization of security software, adequate logical and physical security controls, and adequate reviews of security violations.

3. Proprietary Data, Model Specification and Variable Measurement

3.1 Proprietary Data

The IS audit data used in this study is acquired from a Big 4 firm. The firm granted access to its archived audit working paper records for a given practice office that has a primarily technology client base (high-tech and biotech clients).[5] Using a random number generator, sample audits were selected from the list of archived engagements containing audit files from 1996 to 1999 (pre-dating Sarbanes-Oxley). 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 clients are publicly traded companies. The auditing firm assisted in the coding of variables used in this study.

The extracted workpaper data used in this study includes the following:

- The IS auditor's assessment of whether the client employs an independent security governance function.
- The IS auditor's assessment of whether the client communicates information security policies and procedures to all employees.
- The IS auditor's assessment of whether the client employs information security software.
- The IS auditor's assessment of whether the client employs adequate logical and physical access controls.
- The IS auditor's assessment of whether the client employs adequate reviews of security violations.
- The IS auditor's assessment of whether the client employs an independent security governance function.
- The IS auditor's assessment of the strength of management's security control consciousness.
- The IS auditor's firm-wide (i.e., global) assessment of security control strength.
- The number of years the auditor has been auditing the client.
- The client's total assets.
- Whether the client is publicly or privately held.
- The client's industry classification (either high-tech or biotech).

[5] As a condition to accessing this data we agreed not to disclose the identity of this firm. We retained all rights to publish our findings without any review or approval from the supplying firm.

3.2 Model Specification and Variable Measurement

To test H1 – H6, we employ multiple ordinary least squares (OLS) regressions in the following form:[6]

H1 $FUNCTION_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [1]

H2 $COMM_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [2]

H3 $SW_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [3]

H4 $LOGICAL_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [4]

H5 $PHYSICAL_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [5]

H6 $REVIEW_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [6]

Variable measurement summary:

FUNCTION =1 if the IS auditor has documented that management employs an independent information security governance function.
=0 otherwise.

COMM =1 if the IS auditor assesses that management communicates information security policies and procedures to all employees.
=0 otherwise.

SW =1 if the IS auditor assesses that management has implemented and maintains security software.
=0 otherwise.

LOGICAL =1 if the IS auditor assesses that management implements and maintains adequate logical data access controls.
=0 otherwise.

PHYSICAL =1 if the IS auditor assesses that the client implements and maintains adequate physical access restrictions over servers and CPUs.
=0 otherwise.

REVIEW =1 if the IS auditor assesses that management adequately reviews security violation logs and resolves related security breeches in a timely manner.
=0 otherwise.

MCC =3 if the auditor assess management security control consciousness as 'strong.'
=2 if the auditor assess management security control consciousness as 'moderate.'
=1 if the auditor assess management security control consciousness as 'weak.'

TENURE = a continuous variable representing the number of years the auditor has been auditing the client.

TA = a continuous variable representing the book value of client total assets.

PUB =1 if the client is publicly held.
=0 if the client is privately held.

IND =1 if the client is a high-tech firm.
=0 if the client is a biotech firm.

SEC =3 if the auditor assesses global security control strength as 'strong.'
=2 if the auditor assesses global security control strength as 'moderate.'
=1 if the auditor assesses global security control strength as 'weak.'

[6] While the bivariate dependent variables facilitate the use of logistic regression, our use of OLS conservatively bias us away from statistically significant estimated coefficients. Results using Logistic regression are similar.

The independent variable MCC is the IS auditor's assessment of management security control consciousness, and is our primary variable of interest. The IS 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). The assurances firm guides the IS auditor to make the MCC assessment in a holistic manner based primarily on inquiry of management about the importance of security controls. Additional factors include management's knowledge of the placement and operation of security procedures as well as evidence from an adequate understanding of the client's security control structure. Any relevant security control evidence from other parts of the IS or financial statement audit also may affect MCC.

The IS auditor's workpapers document MCC as "strong," "moderate," or "weak." This assessment is coded 3 for strong, 2 for moderate, and 1 for weak. MCC is expected to obtain a positive coefficient on all the dependent variables presented in Equations 1-6, indicating that management security control consciousness will positively affect the presence of (1) an independent information security governance function (FUNCTION), (2) the communication of information security policies and procedures (COMM), (3) the utilization of security software (SW), (4) logical access controls (LOGICAL) and (5) physical access controls (PHYSICAL), and (6) reviews of security violation logs (REVIEW).

We include several control variables which are discussed next. Prior literature has noted that the length of the auditor-client relationship may affect risk assessments and audit effort due to learning over time (Ashton 1991; O'Keefe, Simunic and Stein 1994). We control for this by including the number of years the auditor has been auditing the client (TENURE). As a result of the audit process, the client should have attained an understanding of control deficiencies to be mitigated. Over time these refinements should result in increased security control procedures, resulting in a positive coefficient on TENURE.

To control for client size, we include the book value of client total 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, we utilize the natural log of total assets. 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 to affect the relationship with security control activities. Accordingly, there is no expectation on the sign on TA.

Prior research suggests the auditor is more likely to be sued if the client 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. We control for this by including an indicator variable (PUB) (Public=1, Private=0), which we expect to exhibit a positive association with security control activities.

To control for potential systematic differences in the manner in which IS audits are conducted between industry groups as identified by the data-granting firm, we include an indicator variable representing the two industry categories in our sample (biotech and high-tech) (IND). Given the lack of evidence concerning major changes in audit approach by the data-granting firm between industry groups, there is no expectation for the coefficient on IND.

3.3 Modified tests of H1-H6

Management may prevent, detect and correct any specific security risk using a variety of control procedures *simultaneously*. Further, any one security control procedure may provide possible crossover risk mitigation (i.e., positive risk mitigation externalities). As an example of simultaneous use of control procedures, both the physical ability to use computer equipment (physical access controls) and the ability to gain access to privy data (logical access controls) work to restrict user access to perform specific functions authorized by management. To address potential simultaneity effects between security control procedures, and to improve the efficiency of the

coefficient estimation, we modified the original tests of H1-H6 by including security control procedures as control variables and employing Seemingly Unrelated Regression (SUR) analysis as follows:[7]

H1 (SUR)
$$FUNCTION_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 COMM_i + \beta_3 SW_i + \beta_4 LOGICAL_i + \beta_5 PHYSICAL_i + \beta_6 REVIEW_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i \quad [7]$$

H2 (SUR)
$$COMM_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 SW_i + \beta_4 LOGICAL_i + \beta_5 PHYSICAL_i + \beta_6 REVIEW_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i \quad [8]$$

H3 (SUR)
$$SW_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 COMM_i + \beta_4 LOGICAL_i + \beta_5 PHYSICAL_i + \beta_6 REVIEW_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i \quad [9]$$

H4 (SUR)
$$LOGICAL_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 COMM_i + \beta_4 SW_i + \beta_5 PHYSICAL_i + \beta_6 REVIEW_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i \quad [10]$$

H5 (SUR)
$$PHYSICAL_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 COMM_i + \beta_4 SW_i + \beta_5 LOGICAL_i + \beta_6 REVIEW_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i \quad [11]$$

H6 (SUR)
$$REVIEW_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 COMM_i + \beta_4 SW_i + \beta_5 LOGICAL_i + \beta_6 PHYSICAL_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i \quad [12]$$

While many potential crossover effects between security control procedures exist, the relationship between them is not intuitive. Therefore, no expectation is held on the signs of the security control procedure coefficients when they are independent variables.

To test H7, a multiple OLS regression is employed in the following form:

H7
$$SEC_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 COMM_i + \beta_4 SW_i + \beta_5 LOGICAL_i + \beta_6 PHYSICAL_i + \beta_7 REVIEW_i + \beta_8 TENURE_i + \beta_9 TA_i + \beta_{10} PUB_i + \beta_{11} IND_i + e_i \quad [13]$$

The dependent variable is the IS auditor's firm-wide (e.g., global) 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 the auditor's summary metric that takes into consideration the strength of the security control environment, systems, policies and control procedures as a whole.[8] Equation 13 extends a similar analysis in Kizirian (2004) with the inclusion of SW, LOGICAL, PHYSICAL, and REVIEW. The coefficient on MCC is expected to obtain a positive value, indicating that strong management security control consciousness will positively affect the IS auditor's global security control strength assessment.

4. Results

Table 1 presents OLS regression results for Equations 1-6 which regress various security control procedures assessed and documented by the IS auditors on our variable of interest, MCC.

[7] For a description of SUR, see Zellner (1962). In addition to FUNCTION and COMM which were studied in Kizirian (2004), this paper has measured and coded the variables SW, LOGICAL, PHYSICAL, and REVIEW. This combined set of variables represents the complete set of security control procedures assessed and documented by the IS auditors in our study, and allows us to run appropriately specified SUR models.

[8] The assessment is conducted in a manner consistent with generally accepted standards (i.e., SAS 94, ISACA 2002).

Table 1
OLS Regression Analysis (N=60)

H1 $FUNCTION_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [1]

H2 $COMM_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [2]

H3 $SW_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [3]

H4 $LOGICAL_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [4]

H5 $PHYSICAL_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [5]

H6 $REVIEW_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 TENURE_i + \beta_3 TA_i + \beta_4 PUB_i + \beta_5 IND_i + e_i$ [6]

Dependent Variables

Independent Variables and Expected Signs		Function	Comm	Sw	Logical	Physical	Review
Intercept		-0.6857	-0.3037	0.3652	-0.4479	-0.6328	-0.2874
		0.1930	0.5510	0.5309	0.4773	0.3793	0.6411
MCC	+	0.4489***	0.5816***	0.4315***	0.3846***	0.2642**	0.3362***
		<0.0001	*<0.0001*	*<0.0001*	*<0.0001*	0.0126	0.0003
TENURE	+	0.0026	-0.0152	0.0085	0.0062	-0.0193	0.0329**
		0.8402	0.2341	0.5594	0.6927	0.2835	0.0357
TA	?	0.0077	-0.0164	-0.0325	0.0130	0.0363	-0.0016
		0.8168	0.6106	0.3807	0.7451	0.4266	0.9673
PUB	+	-0.0208	0.2045	0.0340	0.1127	0.0196	-0.0664
		0.8920	0.1747	0.8424	0.5423	0.9258	0.7137
IND	?	0.0678	-0.0745	-0.0221	-0.1012	0.1303	-0.0869
		0.5167	0.4643	0.8490	0.4218	0.3647	0.4811
Adjusted R-squared		49.62%	56.38%	36.06%	30.83%	13.67%	35.16%

The dependent variables in this table include the assessed presence/absence of an independent security governance function (FUNCTION), communication of information security policies and procedures (COMM), the presence/absence of security software (SW), the presence/absence of adequate logical (LOGICAL) and physical (PHYSICAL) security controls, and the presence/absence of adequate reviews of security violations (REVIEW). The experimental variable, MCC, is the IS auditor's assessed level of management security control consciousness. MCC takes on values of 3, 2, or 1 where 3 indicates a strong level of control consciousness. The control variables include the years as auditor (TENURE), the natural log of total assets (TA), 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 two-tailed.

Consistent with our expectations, MCC obtains significant, positive coefficients when FUNCTION (0.4489, p<0.0001), COMM (0.5816, p<0.0001), SW (0.4315, p<0.0001), LOGICAL (0.3846, p<0.0001), PHYSICAL (0.2642, p=0.0126) and REVIEW (0.3362, p=0.0003) are dependent variables, providing evidence to support H1-H6. These results indicate that, when considered independently, the strength of management security control consciousness, as assessed by the IS auditor (MCC), positively affects the (1) presence of an independent information security governance function (FUNCTION), (2) the communication of information security policies and procedures (COMM), (3) the utilization of security software (SW), (4) logical access controls (LOGICAL) and (5) physical access controls (PHYSICAL), and (6) reviews of security violation logs (REVIEW). Interestingly, the control variables TA, PUB and IND, which are conventionally used in financial statement auditing studies (e.g., O'Keefe et al. 1994) do not obtain statistical significance in this IS audit setting focusing on security controls. Auditor tenure obtains a significant, positive coefficient when REVIEW (0.0329, p=0.0357) is a dependent variable, suggesting that over time the client learned of the importance of adequate reviews of security violations. Equation 1-6 variance inflation factors (VIFs) do not exceed 1.79 indicating multicolinearity does not affect these results.[9]

[9] Marquandt (1980) argues that a multicolinearity problem exists if VIF values exceed 10.

Table 2 presents SUR results for IS auditor-assessed security control procedures on MCC.

Table 2
Seemingly Unrelated Regression Analysis (N=60)

H1 (SUR) $FUNCTION_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 COMM_i + \beta_3 SW_i + \beta_4 LOGICAL_i + \beta_5 PHYSICAL_i + \beta_6 REVIEW_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i$ [7]

H2 (SUR) $COMM_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 SW_i + \beta_4 LOGICAL_i + \beta_5 PHYSICAL_i + \beta_6 REVIEW_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i$ [8]

H3 (SUR) $SW_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 COMM_i + \beta_4 LOGICAL_i + \beta_5 PHYSICAL_i + \beta_6 REVIEW_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i$ [9]

H4 (SUR) $LOGICAL_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 COMM_i + \beta_4 SW_i + \beta_5 PHYSICAL_i + \beta_6 REVIEW_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i$ [10]

H5 (SUR) $PHYSICAL_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 COMM_i + \beta_4 SW_i + \beta_5 LOGICAL_i + \beta_6 REVIEW_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i$ [11]

H6 (SUR) $REVIEW_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 COMM_i + \beta_4 SW_i + \beta_5 LOGICAL_i + \beta_6 PHYSICAL_i + \beta_7 TENURE_i + \beta_8 TA_i + \beta_9 PUB_i + \beta_{10} IND_i + e_i$ [12]

Dependent Variables

Independent Variables and Expected Signs		**Function**		**Comm**		**Sw**		**Logical**		**Physical**		**Review**	
Intercept		-0.9471		-0.2559		0.9106		-0.9272		-0.5533		-0.1961	
		0.0805	*	0.6300		0.1100		0.1376		0.4558		0.7648	
MCC	+	0.5065	***	0.6313	***	0.1296		0.2325		0.1440		-0.0812	
		0.0004		*<0.0001*		0.3954		0.1675		0.4809		0.6522	
FUNCTION	?			-0.0739		0.3407	**	-0.5853	***	0.2505		-0.0480	
				0.5956		0.0230		0.0004		0.1992		0.7805	
COMM	?	-0.0778				-0.2904	*	0.1722		-0.4217	**	0.4584	***
		0.5956				0.0578		0.3075		0.0346		0.0095	
SW	?	0.3119	**	-0.2526	*			0.6226	***	0.2783		0.2967	*
		0.0230		0.0578				*<0.0001*		0.1302		0.0707	
LOGICAL	?	-0.4454	***	0.1245		0.5175	***			0.2012		0.0276	
		0.0004		0.3075		*<0.0001*				0.2359		0.8538	
PHYSICAL	?	0.1347		-0.2155	**	0.1635		0.1421				0.1278	
		0.1992		0.0346		0.1302		0.2359				0.3113	
REVIEW	?	-0.0333		0.3020	***	0.2247	*	0.0251		0.1649			
		0.7805		0.0095		0.0707		0.8538		0.3113			

MCC obtains significant, positive coefficients when FUNCTION (0.5065, p=0.0004) and COMM (0.6313, p<0.0001) are dependent variables, but not when SW (0.1296, p=0.3954), LOGICAL (0.2325, p=0.1675), PHYSICAL (0.1440, p=0.4809), and REVIEW (-0.0812, p=0.6522) are dependent variables, providing evidence to support H1 and H2, but not H3-H6.[10] These results indicate that management security control consciousness (MCC) positively affects the establishment of an independent information security governance function (FUNCTION) and the communication of security policies and procedures to all employees (COMM), while controlling for any potential simultaneity and substitution effects between the security control procedures. Management security control consciousness (MCC) does not appear to *incrementally* affect the implementation and maintenance of security software (SW), logical access controls (LOGICAL) and physical access controls (PHYSICAL), and the review of security violation logs (REVIEW) when controlling for other security control

[10] VIF's do not exceed 6.15 in Equations 7-12. These VIF's are obtained from OLS regressions.

TABLE 2 (Continued)
Seemingly Unrelated Regression Analysis (N=60)

TENURE	+	0.0052	-0.0277	**	-0.0042	0.0062	-0.0354	*	0.0398	**
		0.7096	0.0426		0.7711	0.6927	0.0644		0.0167	
Adjusted R-squared		50.15%†	56.71%†		44.27%†	37.91%†	15.65%†		33.41%†	

Variable Definition:

The dependent variables in this table include the assessed presence/absence of an independent security governance function (FUNCTION), communication of information security policies and procedures (COMM), the presence/absence of security software (SW), the presence/absence of adequate logical (LOGICAL) and physical (PHYSICAL) security controls, and the presence/absence of adequate reviews of security violations (REVIEW). The experimental variable, MCC, is the IS auditor's assessed level of management security control consciousness. MCC takes on values of 3, 2, or 1 where 3 indicates a strong level of control consciousness. The control variables include the years as auditor (TENURE), the natural log of total assets (TA), 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 two-tailed.

† Adjusted R-squared is based on OLS regression, as opposed to the SUR weighted R-squared.

procedures. These results are consistent with the larger independent OLS R-squared values for Equations 1 (FUNCTION, 49.62%) and 2 (COMM, 56.38%) presented in Table 1. Similar to Equations 1-6, the control variables TA, PUB and IND do not obtain statistical significance in the Equations 7-12 SUR analysis, and therefore, while they are included in the SUR analysis, they are not presented in Table 2. Interestingly, Table 2 indicates various security control procedure crossover effects (i.e., possible simultaneous tradeoffs, substitution or control procedure externalities) which are not the focus of this study.

Table 3 presents the Equation 13 OLS analysis regressing MCC on SEC while controlling for a comprehensive set of assessed security control procedures documented by the IS auditor.

Consistent with Kizirian (2004), MCC obtains a significant, positive coefficient (0.4191, p=0.0006), providing evidence to support H7.[11] The control variables TENURE, TA, PUB and IND do not obtain statistical significance in Equation 13, and therefore, while they are included in the regression, they are not presented in Table 3.

5. Summary and Conclusions

Using IS audit workpaper evidence, this study examines and finds that the level of management's security control consciousness directly influences the presence of various assessed security control procedures as well as the IS auditor's global assessment of security control strength. The IS auditor's management security control consciousness assessment measures management's *attitude* toward security controls. The Sarbanes-Oxley Act of 2002 highlights that the establishment of strong management control consciousness (i.e., management's attitude about internal control) is a key factor in the production of accurate and reliable financial information.

When examined independently using OLS analysis, the management security control consciousness assessment is directly associated with the presence of an independent information security governance function, communication of information security policies, utilization of security software, logical access controls, physical access controls, and reviews of security violations.

[11] VIF's do not exceed 6.20 in Equation 13.

Table 3
OLS Regression Analysis (N=60)

H7 $SEC_i = \beta_{0i} + \beta_1 MCC_i + \beta_2 FUNCTION_i + \beta_3 COMM_i + \beta_4 SW_i + \beta_5 LOGICAL_i + \beta_6 PHYSICAL_i + \beta_7 REVIEW_i + \beta_8 TENURE_i + \beta_9 TA_i + \beta_{10} PUB_i + \beta_{11} IND_i + e_i$ [13]

Dependent Variable: Assessed Global Security Controls Strength (SEC)

Independent Variables and Expected Signs			
Intercept		0.6907	
		0.0954	*
MCC	+	0.4191	***
		0.0006	
FUNCTION	+	0.0059	
		0.9559	
COMM	+	0.0932	
		0.4025	
SW	+	0.2699	**
		0.0117	
LOGICAL	+	0.2240	**
		0.0210	
PHYSICAL	+	0.1355	*
		0.0922	
REVIEW	+	0.1411	
		0.1218	
Adjusted R-squared		84.30%	

The dependent variable is the IS auditor's assessed global strength of security controls (SEC), taking on values of 3, 2, or 1, where 3 represents strong levels of control. MCC, is the IS auditor's assessed level of management security control consciousness. MCC takes on values of 3, 2, or 1 where 3 indicates a strong level of control consciousness. The independent variables in this table include the assessed presence/absence of an independent security governance function (FUNCTION), communication of information security policies and procedures (COMM), the presence/absence of security software (SW), the presence/absence of adequate logical (LOGICAL) and physical (PHYSICAL) security controls, and the presence/absence of adequate reviews of security violations (REVIEW). Statistical significance for parameter estimates are indicated at the 1% (***), 5% (**) and 10% (*) levels. All tests are two-tailed.

Due to the possibility that several security control procedures may simultaneously address a single potential security risk, and that several security risks may simultaneously be mitigated by a single security control procedure, Seemingly Unrelated Regression analysis was performed, and additional security control procedures were included as control variables. The Seemingly Unrelated Regression analysis rigorously tests the management security control consciousness – security control procedure relationship. The Seemingly Unrelated Regressions indicate that the management security control consciousness assessment incrementally influences some, but not all security control procedures when remaining security control procedures are added as controls. Results indicate that security control consciousness affects the establishment of an independent information security governance function and the effective communication of information security policies to all employees.

This study further finds that the level of management security control consciousness directly affects the IS auditor's global security control strength assessment. While this finding is consistent with Kizirian (2004), it is also extends that prior literature as it includes a comprehensive set of IS auditor considerations that feed into the global security control strength assessment.

The security control consciousness – control procedure relationship found in this study is consistent with professional guidance and prior literature showing that management control consciousness is a key factor for reliable financial reporting and sound internal control (e.g., D'Aquila 1998; Wong-on-Wing, Reneau and West 1989). Results suggest that IS managers who are security control conscious fund and support security control procedures that are likely to be effective in enhancing control and significantly contributing to the overall security of the information system.

The data is drawn from one specific office of one Big 4 firm, potentially reducing the generalizablity 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.

6. Suggestions For Future Research

The results of this study have implications to IS auditing practice and to future research. The evidence presented suggests that an assessment of management security tone appears to provide important information that improves the IS auditor's decision-making, and is a key consideration in the assessment of global security control strength. The primary focus of the Sarbanes-Oxley Act is data integrity, and data integrity without security controls cannot reasonably be achieved. Auditors working to provide Sarbanes-Oxley Act certification for a systems-dependent organization will benefit from a management security control consciousness assessment. The assessment will likely provide valuable information on whether an information system has effective internal controls in place to produce accurate and reliable financial statements.

The authors wish to thank the assurances firm for their provision of data, and gratefully acknowledge the Department of Accounting at the University of Arizona whose generous support enabled data collection. Comments by Ronny Daigle, Audrey Gramling 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. _____. 1995. "Reports on Audited Financial Statements". *Statement on Auditing Standards No. 79*. New York, NY: AICPA.
3. _____. 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.
4. Ashton, A. H. 1991. "Experience and error frequency knowledge as potential determinants of audit expertise". *The Accounting Review* 66 (April): 218-239.
5. 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.
6. Bakshi, Sunil. 2004. "Control Self-assessment for Information and Related Technology". *Information Systems Control Journal.* Volume 1, 2004.
7. *Control Objectives for Information and related Technology (COBIT)* 3rd Edition. 2002. Copyright © 2002 by the Information Systems Audit and Control Foundation (ISACF).
8. 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: Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992), Internal Control: Integrated Framework: Framework, Coopers & Lybrand, September.
9. D'Aquila J. M. 1988. "Is the control environment related to financial reporting decisions?" *Managerial Auditing Journal*. Volume 13, Number 8. 1998
10. Guldentops, E. 2001. "Harnessing IT for Secure, Profitable Use". *Information Systems Control Journal*, Volume 5, 2001
11. Greene, F. 2002. "A Survey of Application Security in Current International Standards". *Information Systems Control Journal*, Volume 6, 2002

12. ISACA. 2002. "Information Systems Auditing Standards, Guidelines and Procedures". *Information Systems Audit and Control Association (ISACA)*. ISACA Standards © Copyright 2002. Rolling Meadows, IL.
13. 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.
14. Kizirian, T. 2004. "The Influence of Management Tone on Security Control Strength". *Review of Business Information Systems*. V8.1 (January)
15. 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.
16. 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.
17. 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.
18. 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.
19. Tucker, G. 2001. "IT and the audit". *Journal of Accountancy*. American Institute of Certified Public Accountants (AICPA). September 2001.
20. 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.