

Concede or Deny: Do Management Persuasion Tactics Affect Auditor Evaluation of Internal Control Exceptions?

Christopher J. Wolfe CPA, DBA
Mays Business School
Texas A&M University
4353 TAMU
College Station, TX 77845
(979) 845-0964
Email: cwolfe@mays.tamu.edu

Elaine Mauldin CPA, PhD
College of Business
331 Cornell Hall
University of Missouri – Columbia
Columbia, MO 65211
(573) 884-0933
Email: mauldin@missouri.edu

Michelle Chandler Diaz CPA, PhD
Department of Accounting
E.J. Ourso College of Business
Louisiana State University
Baton Rouge, LA 70803
(225) 578-6216
Email: michelle@lsu.edu

December, 2006

We sincerely thank the participating firm for providing participants and expert insights into the audit process. We thank Duane Brandon, Rich Houston, Bill Kinney, Lisa Koonce, Ed O'Donnell, and workshop participants at Louisiana State University, Texas A&M University, University of Missouri-Columbia, and University of South Carolina, for their thoughtful comments. Christopher Wolfe and Michelle Diaz gratefully acknowledge the Mays Business School for providing financial support while completing this research.

Concede or Deny: Do Management Persuasion Tactics Affect Auditor Evaluation of Internal Control Exceptions?

Abstract: In the audit of internal controls over financial reporting, auditors are required to determine whether observed control exceptions signal a systematic deficiency in internal controls or reflect the inherent limitations of internal controls. Standards require this judgment to be based on the magnitude and likelihood of potential misstatements and any compensating controls, independent of management's assessment. However, this paper reports that management's persuasion tactics sometimes work to lower deficiency judgments demonstrating biased judgment that is not overcome by auditors' professional training. In an experiment with 106 senior-level auditors we find that auditors judge control deficiency as less significant when management concedes a minor control problem than when management denies any control problem for information technology (IT) security breaches, but not for manual application control breakdowns. Our results are consistent with IT security breaches being treated as less diagnostic of management's responsibility for control design and compliance than manual application control breakdowns. While IT security breaches are not, in fact, less diagnostic, the perception that they are appears to provide an unconscious cognitive mechanism for persuasion tactics to alter auditor judgments. In addition to providing evidence of systematic bias in auditor judgment, these findings also indicate the rationale for the ubiquitous management persuasion attempts surrounding observed control exceptions – sometimes they work.

Key Words: internal control deficiency, audit judgment, management explanation, security breach

Data Availability: Contact the authors

Concede or Deny: Do Management Persuasion Tactics Affect Auditor Evaluation of Internal Control Exceptions?

I. INTRODUCTION

We study when and how management persuasion tactics reduce auditors' deficiency judgments about observed control exceptions. Deficiency judgments are a critical component of the internal control audit mandated by the Sarbanes Oxley Act of 2002 (SOX) and under-recognized deficiencies can lead to inappropriate internal control reporting or failure to identify needed remediation action. At the same time, auditors' deficiency judgments can be costly to managers. For example, Ashbaugh-Skaife et al. (2005) find that capital markets react negatively to reports of material weaknesses in internal controls and Banham (2006) reports that 60 percent of chief financial officers are replaced within six months after such reports. As a result, managers have strong incentives to try to persuade auditors that observed control exceptions are not deficiencies and anecdotal reports indicate such attempts are pervasive.¹

We study two types of persuasion tactics meant to influence auditor judgment: *concession* that the exception signals an inconsequential exception, but not a control deficiency, and *denial* that the exception signals a deficiency. These tactics should not influence auditor judgment because they are meant to persuade the auditor without providing any new information about the exception. Auditing Standard Number 2 (AS2) requires that auditors' evaluation of control exceptions be independent of management's assessment and be based on the magnitude and likelihood of a financial report misstatement after considering compensating controls (PCAOB

¹ We informally polled over ten Big 4 auditors of various rank in regards to this question and received responses that indicated it was common for clients to take self-serving views of internal control exceptions and attempt to persuade the auditor that the exception is not a deficiency, either by conceding an inconsequential issue or denying the issue. Per AS 2 (PCAOB 2004), a group of lower-level internal control deficiencies can sum to a higher-level internal control deficiency. Therefore, the auditors we polled indicated that manager concern is not strongly limited by a materiality threshold, and managers tended to challenge any level of potential control deficiency.

2004). AS 2 also recognizes that internal controls are inherently fallible such that auditors must determine whether observed control exceptions are attributable to a systematic breakdown in controls or to underlying limitations in internal controls (PCAOB 2004 ¶ 12). The potential fallibility of controls provides the opportunity for management persuasion tactics to work.

Prior research in psychology finds that different persuasion tactics are more or less effective in different contexts because they work through different cognitive mechanisms and have different advantages and disadvantages. The advantage of a concession is that it indicates acceptance of responsibility (Bottom et al. 2002; Kim et al. 2004; Ohbuchi et al. 1989; Schwartz et al. 1978) and the disadvantage is that it admits that the event could have been prevented. The reverse holds for denial where the advantage is that it can create distance between an event and the accused party and the disadvantage is that it indicates a lack of acceptance of responsibility (Kim et al. 2004). A persuasion tactic's effectiveness depends on whether its advantages outweigh its disadvantages in a given context (Kim et al. 2006; Shaw et al. 2003). Kim et al. (2004) find concessions are more effective than denials for weakly diagnostic failure events, suggesting that the effectiveness of persuasion tactics in our setting depends on how diagnostic auditors perceive a given exception to be of a systematic internal control deficiency.

We study the effects of persuasion tactics for two regularly occurring types of internal control exceptions that can both lead to financial misstatement and are both preventable with proper controls and compliance, but that are expected to vary with respect to their perceived diagnosticity: IT security breaches and manual application control breakdowns.² IT security

² IT security breaches involve inappropriate use of a firm's information system whereby firm data is changed and/or illicitly used. Most security breaches are caused by employee failure to follow control procedures (Gansler and Lucyshyn 2005). Manual application control breakdowns involve exceptions within a particular application (e.g., accounts receivable) and are also based upon employee failure. All control exceptions in this research are based upon employee failures. IT security breaches can be classified as application control breakdowns or pervasive control breakdowns dependent on whether the control is designed to protect single or multiple applications.

breaches are technology-enabled and more easily attributed to external forces. Attribution theory indicates that each of these contextual features is associated with cognitive perceptions of reduced diagnosticity of causal control and reduced management responsibility (Naquin and Kurtzberg 2004; Wood and Mitchell 1981). For IT security breaches, we expect management concession will be persuasive because concession capitalizes on the advantage of accepting responsibility with little or no disadvantage from admitting a connection to a control breakdown that is only weakly diagnostic of management responsibility. Since manual application control breakdowns do not have characteristics that deflect attributions and a concession confirms that management is responsible for the breakdown, we do not expect concession will be persuasive for manual application control exceptions. We expect denial is an ineffective strategy regardless of perceived attribution for the exception because denial indicates an unwillingness to accept responsibility, and it is not credible to deny a connection between an observed control exception and any level of control deficiency.

One hundred six senior-level auditors from a Big 4 public accounting firm evaluated internal control exceptions based on a case study, including a vignette conversation between the audit senior and management. We manipulated, between auditors, management's persuasion tactic (concession or denial) and the control exception context (IT security breaches or manual application control breakdowns³). To confirm that IT security breaches are perceived less diagnostic of systemic internal control problems, we find that the auditors blamed management less for IT security breaches than for manual application control breakdowns.

³ Following AS 2 (PCAOB 2004) and the framework for evaluating control exceptions (BDO Seidman LLP et al. 2004) all control exceptions had a direct effect on the financial statements.

For IT security breaches, we find, as expected, that auditors judge management's explanation as more adequate and the control deficiency lower when management concedes an inconsequential problem than when management denies the existence of any control problems. These findings are consistent with reduced professional skepticism and are further explained in a path model. For IT security breaches, our path model indicates that management concession increases perceived explanation adequacy and that higher perceived explanation adequacy reduces control deficiency judgments both directly and indirectly through judgments of the magnitude and likelihood of financial misstatement. For manual application control breakdowns, we find, as expected, persuasion tactics had no effect on perceived explanation adequacy or control deficiency judgments, even though the path model reveals substantially identical effects of perceived explanation adequacy, compensating controls, magnitude of misstatements and likelihood of misstatements on control deficiency judgments.

Our results have implications for both practice and theory. For practice, audit firms are concerned that internal control audits are conducted consistently and without bias. As in any new work, prior to improving decision-making, it is necessary to know in what areas judgment is deficient. Our study provides evidence of systematic bias in auditor judgment in adhering to requirements of AS 2. Theoretically, our results add to the audit explanation literature by indicating that persuasion tactics, distinct from management's incentives and the content of the explanation itself, can have a significant effect on auditor judgment dependent on the way they are communicated and the context in which they are offered. Thus, our study provides a more complete picture of the complex relationship between management explanations and auditor judgments.

The remainder of the paper is organized as follows. The next section reviews prior literature and develops the theoretical basis for our hypotheses. Then, the experimental methods are described and the results are presented. We conclude with a summary and discussion of our study's implications and limitations.

II. BACKGROUND AND HYPOTHESES

Our study is most closely related to prior literature on management's self-serving explanations. Findings indicate that management makes self-serving explanations in annual reports (Aerts 2005; Barton and Mercer 2005; Bettman and Weitz 1986) and to auditors when defending their position related to earnings management attempts (Nelson et al. 2002). This literature supports the notion that management is likely to make self-serving explanations to persuade the auditor that observed internal control exceptions are not a result of deficiencies in internal controls.

Explanation research also indicates that incentives and content influence the persuasiveness of management explanations. Anderson et al. (2004) find that auditors are less persuaded by self-serving explanations when management has incentives to manage earnings. Barton and Mercer (2005) find that only plausible explanations for unfavorable outcomes persuade analysts. Research in the internal control audit setting finds that mere knowledge of management's self-assessment of internal controls influenced auditors' judgments (Arel et al. 2006; Earley et al. 2006). We extend this literature through an examination of persuasion mechanisms embedded in management explanations offered to auditors. A rich psychology literature indicates different persuasion tactics are available to explain failure, and their relative effectiveness is determined by unconscious and spontaneous attribution evaluations dependent on the context of the failure event (Shaw et al. 2003). We develop expectations about the interaction between persuasion

tactics and context on auditors' judgments in the audit of internal controls over financial reporting.

The Audit of Internal Controls over Financial Reporting

AS 2 provides standards for the audit of internal controls over financial reporting mandated by SOX. We focus on the auditor's evaluation of internal control exceptions found during tests of operating effectiveness because this evaluation is a critical component of the audit (PCAOB 2004 ¶ 127, 129). An internal control exception that is determined to be more than inconsequential is classified as a control deficiency, a significant deficiency or a material weakness. Though only material weaknesses directly result in an adverse audit opinion, a group of control deficiencies can accumulate to become a significant deficiency, and a group of significant deficiencies can accumulate to become a material weakness (PCAOB 2004 ¶ 130). Significant deficiencies that remain uncorrected after a reasonable period of time can also result in an adverse opinion (PCAOB 2004 ¶ 10, 140). Further, the auditor must report all significant deficiencies to the audit committee and inform the audit committee when they communicate any control deficiencies to management (PCAOB 2004 ¶ 207, 209). Therefore, control exceptions create concern for both auditors and management, even though individually such control exceptions may not be the basis for an adverse opinion.

The standards in AS 2 require the auditor to determine the likelihood and magnitude of a potential misstatement (PCAOB 2004 ¶ 131), considering both quantitative and qualitative factors (PCAOB 2004 ¶ 130). Further, it is the potential for misstatement that must be considered, not whether a misstatement has actually occurred (PCAOB 2004 ¶ 132). Finally, the standards require consideration of a number of other factors, such as compensating controls ((PCAOB 2004 ¶ 133-141). Clearly, the judgment of the significance of a deficiency is complex

and subjective (Boury and Spruce 2005; Heuberger and Nepf 2005). In addition, uncertainty surrounds the signal an observed control exception sends regarding the effectiveness of internal controls. AS 2 states: “Even well-designed controls that are operating as designed might not prevent a misstatement from occurring.” (PCAOB 2004 ¶ 12). Determining whether an observed control exception is diagnostic of a systematic break-down in internal control, attributable to management, or is merely an underlying limitation of internal controls is a key judgment in the evaluation process.

The process for auditor evaluation of internal control exceptions includes inquiry of management to ensure an understanding of the causes and results of the exception, particularly in regards to the frequency of exceptions and compensating controls (PCAOB 2004 ¶ 95). In response to auditor inquiry about internal control exceptions, the opportunity arises for management to persuade the auditor that the exception does not signal a deficiency.

Management’s Persuasion Tactics – Concessions and Denials

Although all self-serving explanations have the same objective of deflecting negative response to failure events, different tactics are available. The uncertain, complex, and subjective nature of the judgment of internal control deficiency suggests that management can plausibly deny that the control exception signals a control deficiency or concede it is an inconsequential exception that should not be classified as a control deficiency. In either case, management implies that the exception does not represent a systematic break-down in internal control, attributable to management. However, neither concession nor denial should influence auditor judgment because they are a persuasion tactic, not new information.

Concessions and denials operate through different mechanisms to change perceptions of the recipient. Concession acknowledges the event, accepts responsibility and indicates regret,

whereas denial maintains distance from the event (Tata 2002; Schonbach 1990). Each has advantages and disadvantages. The advantage of a concession is that acceptance of responsibility and indicating regret heightens perceptions of trust and reduces aggression toward perpetrators (Bottom et al. 2002; Kim et al. 2004; Ohbuchi et al. 1989; Schwartz et al. 1978). The disadvantage of a concession is that acknowledging the event and accepting responsibility implies the accused party could have prevented the event. The advantage of a denial is that it can create distance between the event and the accused party, leading individuals to give the accused party the benefit of the doubt. The disadvantage is that a denial does not indicate acceptance of responsibility and need to rectify behavior, lowering perceptions of trust (Kim et al. 2004).

Prior research finds that the relative weighting of advantages and disadvantages is dependent on failure diagnosticity, an important contextual feature of many failure events. For example, Kim et al. (2004) find that a weakly diagnostic failure event is best repaired with concession as opposed to denial.⁴ Conversely, they find that a denial is most effective for repairing trust in a strongly diagnostic failure event. Failure diagnosticity (indicative of systematic internal control deficiencies attributable to management) is a basic component of the deficiency judgment that we expect will vary across different types of control exceptions. Therefore, we expect an interaction between persuasion tactics and type of internal control exception.

Interaction Effects – Persuasion Tactics and Type of Internal Control Exception

We examine IT security breaches and manual application control breakdowns because theory suggests that these control exceptions are perceived differentially diagnostic of systematic internal control deficiencies. IT security breaches are technology-enabled and more easily

⁴ Kim et al. (2004) refer to apologies, not concessions. However, concessions are considered elaborate apologies (Goffman 1967), because they acknowledge occurrence of the failure event, accept responsibility, and express remorse (Tata 2002). Therefore, we consider equivalently literature studying apology and concession.

attributed to external forces. Psychology research indicates that each of these features commonly lead to biased diagnosticity judgments, providing the cognitive mechanism for the relative advantages of concession to outweigh the relative advantages of denial.

First, prior research demonstrates that external influences are perceived to reduce the diagnosticity of causal control. For example, Wood and Mitchell (1981) find that nurse managers assigned less blame when they could externalize reasons for patient care errors. Weiner (1987) finds through a group of empirical studies that external attributions reduced both anger and tension in inflammatory situations. Finally, Crant and Bateman (1993) find that external attributions reduced the blame placed on guilty staff by audit seniors.

IT security breaches often originate through external parties. For example, *The Wall Street Journal* commonly reports incidents of external penetration of IT security controls (Fields 2006; McQueen 2006; Pacelle and Sidel 2005; Rapoport 2005; Richmond 2005; Cullen 2006; Young 2006; Hechinger 2006; Sidel 2006). Importantly, research and theory demonstrate that properly designed and implemented IT security controls can protect firm data and assets from third-party perpetrators (ITGI 2005). In fact, just as in manual application controls, employees are recognized as the weakest link in the operation of IT security controls (Gansler and Lucyshyn 2005). However, the ability to externalize IT security breaches suggests that management will be held less accountable for IT security breaches than for manual application control breakdowns.

Second, prior research finds that technology reduces the perceived diagnosticity of causal control. Naquin and Kurtzberg (2004) theorize that though every negative incident is caused by a sequence of interrelated antecedent events, these events are easier to analyze when human error alone is involved than when technology is involved. Following attribution theory, they posit that negative events involving technology are perceived as less controllable than those involving

human error, because it is easier to imagine discretionary activities related to humans than to technology. Resulting from these differential perceptions, Naquin and Kurtzberg (2004) hypothesize and find that individuals attribute less accountability to the organization when an accident involves technology than when it involves only human error. Importantly, they note that these perceptions are in spite of the fact that “we install technological control into our lives at astounding rates for exactly this reason – to avoid the inevitable mishaps associated with error-prone human behavior” (Naquin and Kurtzberg 2004, 131). Given that IT security breaches are technology-based, the findings of Naquin and Kurtzberg (2004) offer further evidence that management will be held less accountable for IT security breaches than for manual application control breakdowns.

Since IT security breaches are expected to be perceived less diagnostic of systematic internal control deficiencies, concession reaps the advantage of heightened perceptions of trust and reduced aggression while the disadvantages are minimized. Even though management acknowledges connection to the event, the exception itself is already perceived anomalous. On the other hand, the disadvantages of a denial are greater than the advantages. The denial lowers perceptions of trust by not accepting responsibility and receives no additional benefit from creating doubt since weak diagnosticity already creates doubt. Therefore, we predict a concession to be more effective than a denial in ability to influence for IT security breaches.

Since manual application control breakdowns are expected to be perceived as more diagnostic of systematic problems, conceding is not effective because it confirms that management is responsible for a control exception that could have been prevented. In an internal control audit, the advantage of denial is not effective either, because disconnecting management from a highly diagnostic event is not credible. We predict no difference in ability to influence

between a concession and a denial for manual application control exceptions. We test ability to influence using perceived explanation adequacy because psychology research indicates that explanation adequacy is a key perception underlying the ability of explanations to positively influence the recipient of the explanation (Shaw et al. 2003). Accordingly, our first hypothesis is stated as follows.

H1: For IT security breaches, perceived *explanation adequacy* will be higher when management embeds concession-based persuasion tactics in their explanation of the breach as compared to embedding denial-based persuasion tactics in their explanation, but there will be no difference in the perceived *explanation adequacy* for manual application control exceptions regardless of whether management embeds concession or denial-based persuasion tactics in their explanation of the exception.

The more adequate an explanation is perceived to be the greater its ability to mitigate negative reactions (Shaw et al. 2003). Yet, AS 2 requires the auditor to make their judgments based on an attitude of professional skepticism, essentially involving a critical assessment of management (PCAOB 2004 ¶ 36). Auditors practicing professional skepticism should not be swayed by management's persuasion tactics. However, if an auditor's perception of the adequacy of management's explanation is affected by self-serving persuasion tactics as predicted, the implication is that auditors are not practicing professional skepticism to the degree required. In the setting studied, reduced professional skepticism is expected to lead to auditor judgments that favor management's position regarding the significance of the potential control deficiency.

Accordingly our second hypothesis is as follows:

H2: For IT security breaches, auditor judgment of the *significance of control deficiency* will be lower when management embeds concession-based persuasion tactics in their explanation of the breach as compared to embedding denial-based persuasion tactics in their explanation, but there will be no difference in auditor judgment of the *significance of control deficiency* for manual application control exceptions regardless of whether management embeds concession or denial-based persuasion tactics in their explanation of the exception.

Because auditors are specifically trained in both internal control structure and the application of professional standards, it could be argued that they will not fall prey to attribution biases triggered by the context in which the judgment is made. As Joyce and Biddle (1981) point out, biases found in individuals in basic psychology research are not always found in auditors. Since Alicke (2000) suggests that attributions are influenced by relatively unconscious, spontaneous evaluations, we expect that auditors will not overcome these psychological biases.

III. RESEARCH METHODS AND PARTICIPANTS

To test our hypotheses, we conducted an experiment where audit seniors evaluated two internal control exceptions after reading a manager's explanation for the exceptions. Management's persuasion tactic (concession or denial) and the type of internal control exception (IT security breaches or manual application controls) were varied between participants.

Experimental Task and Materials

The task required participants to read a case and then assess two internal control exceptions. Materials consisted of background information about a manufacturing company, summary financial statements, a narrative description of the company's revenue transaction processing cycle, information concerning auditor observed control exceptions, and a conversational vignette between an auditor and a client manager. All exceptions were designed such that they could have potentially contributed to a more than inconsequential misstatement of the financial statements and the root cause was employee failure to follow procedures. Control exceptions were manipulated as IT security breaches or manual application control breakdowns. In the IT security breach condition, the first exception involved a password policy violation resulting in placement of false sales orders from a stolen laptop. The second exception involved a system breach where an employee wrongly provided access to an intruder who stole customer procurement card

information. In the manual application control exceptions condition, the first exception involved inappropriate credit approval overrides and the second issue involved unrecorded discounts on sales. To ensure that our findings are not driven by idiosyncrasies in one exception and yet still keep the analyses tractable, each participant analyzed two internal control exceptions; either the two IT security breaches or the two manual application control breakdowns. See Appendix A for an excerpt of the experimental materials that describes the control exceptions.

The conversational vignette took place between the audit senior on the engagement and the client's controller. In the vignette, the controller provides explanations for the control exceptions, including either a concession or a denial. See Appendix A for excerpts from the vignettes that present the persuasion tactic manipulations. In the concession (denial) condition, the controller concedes (denies) that there was an operating effectiveness breakdown with respect to each control exception. Importantly, in neither the concession nor the denial treatment does the controller offer to make any changes to internal control procedures, and in each treatment, the controller indicates that management is very concerned with maintaining strong internal controls and that "nothing has occurred that caused a material misstatement of profits," strongly implying that the internal control exceptions should be considered negligible.

Participants were randomly assigned to one of the two types of internal control exception conditions and one of the two persuasion tactics conditions. Within treatment cells, the order of the two internal control exception cases was counterbalanced. Experimental administrators read a script introducing the experiment to the participants, and they distributed envelopes containing an information sheet, general instructions, background questions, and experimental task materials. Administrators also monitored completion of the task and collected the instruments. The experiment was completed in a one-hour period.

Variables

Independent variables adhered to our experimental design and were coded as dichotomous variables including type of exception (IT security breach versus manual application control breakdown), type of persuasion tactic (concession versus denial) and control exception case (first exception versus second exception). Dependent and control variables were measured based on participants' answers to a series of questions for each of their two internal control exceptions. All responses were captured on 11-point scales. The two primary dependent variables are the perceived explanation adequacy and the perceived level of control deficiency signaled by the exception. Perceived explanation adequacy was assessed on a scale with anchors that ranged from "not adequate" to "very adequate." Perceived control deficiency was assessed on a scale with anchors that ranged from "no deficiency" to "significant deficiency."

Control variables for each internal control exception analyzed followed professional guidance in AS 2 regarding the determination of control deficiency. We captured perceptions of the efficacy of compensating controls, the potential magnitude of financial misstatement stemming from the internal control exception, and the likelihood of financial misstatement stemming from the internal control exception. The scale measuring the influence of compensating controls ranged from "negatively influenced" to "positively influenced".⁵ The magnitude of misstatement scale ranged from "inconsequential" to "material", and the likelihood of misstatement scale ranged from "remote" to "probable," consistent with AS 2 terminology. We also capture and report a measure of management blame to verify that differential attributions exist between IT security breaches and manual application control exceptions.

⁵ The 11-point scale on the compensating controls question ranged from -5 to 5, because it encompassed both negative and positive perceptions. All other questions have scales ranging from 1 to 11.

Participants assessed management's blame for a control exception using scale anchors ranging from "no blame" to "all blame".

Participants

Participants were 110 audit seniors from one Big-4 firm attending a national training session for senior-level auditors. Four participants were dropped due to incomplete responses so our final sample consisted of 106 auditors. Table 1 Panel A presents a profile of the participants' experiential backgrounds. As shown, the auditors in our study had an average of about three years of experience; most had been trained on SOX 404 and AS 2 (89.62%); and most had been involved in SOX 404 audits (86.79%). Table 1 Panel B presents the auditors' assessment of control exceptions. The auditors indicated that they understood the control exceptions in the experimental materials, rating understandability between 8.68 and 9.46 on an 11-point scale for each internal control exception. Further, each control exception was perceived as having financial statement implications with consideration of financial statement risk rated between 7.93 and 8.78 on an 11-point scale for each control exception. In sum, the senior auditors who participated in our study appear to have had sufficient background to analyze the control exceptions that they were given, and they considered the exceptions a threat to the integrity of the financial statements. Based on Chi-square and ANOVA testing, we find that the experience and control exceptions assessment metrics were not significantly different ($p > .10$) across treatment conditions with the exception of months of audit experience ($p = .02$).⁶ Each of the experience and control exceptions assessments was included as a covariate in each of the

⁶ Five auditors reported audit experience of 90 to 120 months. If we consider them outliers and drop them from our analyses months of audit experience is no longer significantly different across treatment conditions ($p = .177$). Dropping these auditors from our sample and re-running our statistical analyses produced results substantially identical to those reported. They are, therefore, left in the sample.

multivariate data analyses presented. None were statistically significant or had a substantive effect on the reported results.

[Place Table 1 about here.]

Experimental Checks

To ensure that the internal control exceptions and dialogue were realistic and representative of practice, experimental materials were reviewed by two audit managers (from a Big 4 firm not providing participants), a former Big 4 audit partner, the controller of a publicly traded firm, and they were pilot tested on senior auditors from several different firms. The final versions of the experimental materials were reviewed by a partner and manager from the firm that provided participants to ensure that terminology was consistent with firm terminology and to ensure that the experimental task was appropriate for the firms' senior auditors. While reviewers noted that final determination of internal control deficiencies is made at a higher level than senior auditor, they also indicated that control issues are first analyzed by the engagement senior and they consider these initial assessments of internal control exceptions to be vital to the audit.

Manipulation check questions were included to verify that participants read and understood the treatments. One question asked when the control exception was discovered and was anchored by "while testing revenue cycle application controls" and "while testing information technology general controls." The mean responses of participants in the manual application control exception treatment were 3.07 and 2.50 for the two internal control exceptions. The mean responses of participants in the IT security breach treatment were 8.59 and 8.85 for the two internal control exceptions. All differences between the treatments are statistically significant ($p < .01$). Another manipulation check question asked about the tone of the explanations given by the controller and was anchored on "admitting there was a breach of control" and "denying there

was a breach of control.” The mean responses of participants in the concession treatment were 4.51 and 4.71 for the two internal control exceptions. The mean responses of participants in the denial treatment were 9.98 and 9.78 for the two internal control exceptions. Again, all differences between treatments are statistically significant ($p < .01$) and suggest that participants understood the persuasion tactic employed by the controller. Finally, all participant responses were captured under two different question orders and we observed no order effects. We deem the experimental manipulations and the collection of auditor responses successful.

To verify that IT security breaches are perceived as less diagnostic of management failure to properly design and operate internal controls than are manual application control breakdowns, we analyzed the amount of blame auditors ascribed to management for each exception. Consistent with theory, and as shown in Table 2, the mean level of blame assigned to management is lower for the IT security breaches than for the manual application control breakdowns (password policy violation = 6.04; wrongly granting system access = 8.07; unapproved credit = 9.60; unrecorded discounts = 8.87). To control for the possibility that blame differences are due to the perceived severity of the control exceptions, we also performed a multivariate test. We first regressed management blame on assessed compensating controls, the magnitude of misstatement, and the likelihood of misstatement stemming from the control breakdown. We then used the error terms of that regression as the dependent variable in a repeated measures ANOVA model. As shown in Table 2 panel B, the repeated measures ANOVA results validate the univariate results; the main effect of IT/manual control exceptions

on the management blame dependent variable is statistically significant ($p < .001$, two-tailed).⁷ As expected, auditors perceived IT security breaches as less diagnostic of management failure.

[Place Table 2 about here.]

IV. RESULTS

H1 predicts that perceived explanation adequacy will be higher when management embeds concession-based persuasion tactics in their explanation as opposed to embedding denial-based persuasion tactics in their explanation, for IT security breaches but not for manual application control breakdowns. Table 3 presents t-tests of mean differences between concession and denial treatments for all dependent and control variables. With respect to IT security breaches, mean explanation adequacy perceptions in the concession and denial treatments are 6.22 and 4.22 ($p = .022$, two-tailed) under the password policy exception and 6.19 and 3.14 ($p < .001$, two-tailed) under the wrongly granting system access exception. With respect to manual application control exceptions, mean explanation adequacy perceptions in the concession and denial treatments are 4.26 and 3.79 ($p = .515$, two-tailed) under the unapproved customer credit exception and 3.14 and 3.58 ($p = .510$, two-tailed) under the unrecorded sales discount exception. These univariate t-test results are consistent with H1.

[Place Table 3 about here.]

⁷ In this model, the interaction between IT security breach and the control exception case is significant. This is the result of auditors perceiving significantly less management blame in one of the two IT security breaches (password policy violation). However, as shown in Table 2 Panel A, perceived management blame for each of the two IT security breaches is still significantly less than each of the two manual exceptions ($p < .05$, two-tailed) such that the main effect holds across both exceptions. Additionally, we ran regressions using Huber-White corrected standard errors with blame as the dependent variable; our treatments, control exception cases and their interactions as independent variables; and perceptions of compensating controls and the magnitude and likelihood of misstatement as covariates. Huber-White correction accounts for intraclass correlation between observations from the same sampling unit by adjusting estimates of standard errors (Stata Press 2005). This regression produced substantially identical results to the repeated measures ANOVA presented in Table 2 Panel B.

To validate the univariate t-test findings for perceived explanation adequacy, a repeated measures ANOVA model was estimated (see Table 4 Panel A). Results indicate a significant interaction effect ($p=.004$, two-tailed) between IT security breach/manual application control exception treatments and concession/denial treatments.⁸ The interaction is presented graphically in Figure 1 Panel A. As indicated on the graph, the mean contrast for perceived explanation adequacy between the concession and denial treatments is statistically significant for IT security breaches (2.389; $p<.001$, two-tailed), but the corresponding mean contrast for manual application control exceptions is not statistically significant (0.053, $p=.929$, two-tailed). These results are consistent with H1 and indicate that persuasion tactics, divorced from any evidence in the explanation, affect an auditor's perception of the adequacy of management's explanation for IT security breaches, but not for manual application control breakdowns. Increased perceived explanation adequacy due to a persuasion tactic represents a lapse in professional skepticism. Such a lapse has the potential to lead to audit judgments that are more consistent with management's agenda.

[Place Table 4 and Figure 1 about here.]

H2 predicts that the significance of a control deficiency will be judged lower when management embeds concession-based persuasion tactics in their explanation as opposed to embedding denial-based persuasion tactics, for IT security breaches but not for manual application control breakdowns. As shown in Table 2 and consistent with H2, mean control deficiency judgments in the concession and denial treatments are 5.74 and 7.30 ($p=.027$, two-tailed) under the password policy exception and 8.00 and 9.26 ($p=.042$, two-tailed) under the

⁸ We ran regressions for each dependent variable using Huber-White corrected standard errors. This corrects for intraclass correlation between observations from the same sampling unit by adjusting estimates of standard errors (Stata Press 2005). These analyses produce substantially identical results.

wrongly granting system access exception. For manual application control exceptions, mean control deficiency judgments in the concession and denial treatments are 8.54 and 8.58 ($p=.934$, two-tailed) under the unapproved customer credit exception and 8.43 and 8.13 ($p=.565$, two-tailed) under the unrecorded sales discount exception.

We again use a repeated measures ANOVA model as a multivariate validation of the univariate results for the control deficiency dependent variable. The ANOVA results indicate a significant interaction effect between IT security breach/manual application control exception treatments and concession/denial treatments (Table 4 Panel B, $p=.038$, two-tailed). The graph of the interaction (Figure 1 Panel B) shows that the mean contrast between concession and denial for IT security breach deficiency judgments is statistically significant (1.407, $p=.014$, two-tailed), but the corresponding contrast for manual application controls is not statistically significant (0.128, $p=.789$, two-tailed), consistent with H2. Management persuasion tactics, independent of new information, affect an auditor's judgment of the significance of a control deficiency for IT security breaches, but not for manual application control breakdowns.

Additional Analyses

Theoretically, we argue that if management embeds a self-serving persuasion tactic devoid of information content in an explanation made to an auditor, and due to this, the explanation becomes more effective, then the agenda in management's self-serving explanation will be reflected in auditor judgment. Our separate analyses of explanation adequacy and control deficiency judgments support this logic. However, the separate analyses do not directly inform our theoretical logic. Therefore, we estimate two identical path models, one for IT security breaches and one for manual application control breakdowns to analyze the relationship between concession/denial persuasion tactics, perceived explanation adequacy, and control deficiency

judgments. Our models also include the perceived effectiveness of compensating controls, magnitude of misstatement, and likelihood of misstatement as intervening variables, because AS2 requires that control deficiency be based on these parameters and it is unclear whether these parameters fully mediate the effects of concession/denial persuasion tactics and perceived explanation adequacy on control deficiency judgments.

The path models are shown in Figure 2. Both models contain all statistically significant paths and both models indicate good fit (comparative fit index (CFI) > 0.96 and the standardized root mean square residual (SRMR) < 0.057 for both models) (Kline 2005). Considering first the model for IT security breaches (Figure 2 Panel A), we find that explanation adequacy fully mediates the effect of concession/denial persuasion tactics on control deficiency judgments. This finding validates our theoretical logic that the persuasion tactic reduced professional skepticism (i.e., management's self-serving explanation became more effective) and that the reduction in skepticism was the causal factor that influenced control deficiency judgments. The observed mediation indicates that concession/denial persuasion tactics only influence control deficiency judgments indirectly, and we observed three statistically significant indirect paths leading to the control deficiency judgment: 1) concession/denial => explanation adequacy => control deficiency (0.568, p=.016, two-tailed); 2) concession/denial => explanation adequacy => magnitude of misstatement => control deficiency (0.297, p=.021, two-tailed); and 3) concession/denial => explanation adequacy => likelihood of misstatement => control deficiency (0.258, p=.029, two-tailed). With respect to the path model for manual application control exceptions (Figure 2 Panel B), we find no effect for concession/denial persuasion tactics on perceived explanation adequacy or control deficiency judgments, but the relationship between perceived explanation adequacy

and compensating controls, magnitude of misstatement, likelihood of misstatement, and control deficiency judgment is substantially identical to that in the path model for IT security breaches.

[Insert Figure 2 about here]

Our path model results offer two important insights. First, auditor perception of the adequacy of management's explanation directly affects audit judgment of control deficiency regardless of whether the context is an IT security breach or a manual application control breakdown. This is important, because the professional guidance in AS2 indicates that auditor judgment of a control deficiency should be a function only of the effectiveness of compensating controls and the potential magnitude and likelihood of misstatement stemming from the deficiency. Yet our results indicate a strong, independent effect on auditor judgment based on how adequate management's explanation of the potential control deficiency is perceived. This finding indicates that anything management can do to make their explanations appear more adequate to the auditor will result in audit judgments that are more aligned with management's agenda, and this is the source of the second important insight provided by the path model. We find that dependent on context, persuasion tactics can influence auditor perceptions of the adequacy of management's explanations and ultimately auditor judgments of control deficiency.

V. DISCUSSION

In our experiment, 106 senior auditors evaluated internal control exceptions stemming from either IT security breaches or manual application control breakdowns crossed with either concession or denial-based persuasion tactics embedded in management's explanation of the control exception to the auditor. We find that when management conceded that an IT security breach signaled a minor internal control system problem, auditors assessed explanation adequacy higher and control deficiency lower than when management denied that the security breach

signaled internal control system problems. On the other hand, for manual application control breakdowns, management's persuasion tactics had no differential effect on auditor assessment of control deficiency or explanation adequacy.

Our results indicate that auditors can be influenced by management persuasion tactics for certain types of internal control exceptions. We also find that the auditors blamed management less for breakdowns in IT security than in manual application controls consistent with prior psychology research and indicating that auditors perceive negative events involving IT security to be less diagnostic of systemic internal control problems attributable to management. Reduced diagnosticity provides a mechanism for persuasion tactics to be effective. This is important, because IT controls are available to protect against external penetration and digital theft (ITGI 2005) – yet, at some level, management was forgiven for these breaches when management offered a concession. A conciliatory statement by management offers no assurance of future behavior and such a statement should not systematically affect auditor judgment with respect to current assessment of the client's control system. In fact, inadequate recognition of control deficiencies can lead to failure to remediate controls.

For regulators, our study provides evidence about auditor judgments in adhering to the recently promulgated requirements of AS 2 (Heuberger and Nepf 2005). When a client offers an explanation to an auditor, perceived explanation adequacy imparts a strong independent effect on the ensuing auditor judgment, beyond, and distinct from, its effect on the underlying factors that AS2 indicates should be the basis for a control deficiency judgment, i.e. compensating controls, magnitude of misstatement, and likelihood of misstatement. It appears that auditors do not base control deficiency judgments on only the parameters outlined in AS2 – regardless of the type of control breakdown. With regard to audit practice, our results indicate that a consistent use of

concession-based persuasion tactics in management explanations to auditors is an optimal strategy, because concession-based persuasion tactics are not perceived negatively by auditors and sometimes they produce auditor judgments that are significantly more favorable to management's agenda. This represents a potential bias in an audit judgment that firms should consider addressing in training.

Finally, we extend the management explanation literature to consider persuasion tactics with a primary purpose of deflecting culpability, as opposed to explanations solely for the purpose of offering causal evidence germane to the audit. We demonstrate that the effectiveness of self-serving management explanations depends on persuasion tactics, in addition to management's incentives and the content of the explanation itself. By demonstrating the importance of interaction effects between persuasion tactics and their context, we provide a more complete understanding of the complex relationship between management explanations and auditor judgment.

This research has limitations. Audit planning materials are rich, but they are necessarily restricted in this study due to limits on access to the experimental participants and potential maturity effects in our experiments. Our participants came from one Big 4 firm, and they were all at the senior level. Therefore, our results are specific to senior auditors and potentially specific to the firm that provided the participants. Also, audits usually involve an audit team, and the ability to consult team members can affect audit judgments. In this experiment, we used individual judgments that do not capture dynamic team interactions. However, the initial judgments made and documented by senior auditors have been shown to influence the judgments of reviewing auditors (Ricchiute 1999). Further, the senior auditor participants were experienced in assessing control exceptions, and firm partners indicated that they were capable of assessing

internal control exceptions and that their individual judgments were important to the audit.

Finally, our focus on individual judgments is consistent with prior research in audit judgment and decision-making.

Requirements of SOX have significantly expanded audits of publicly traded firms. Further, audit opinions on internal controls emanating from these requirements affect firms and managers (Ashbaugh-Skaife et al. 2005; Banham 2006). Given the high level of auditor judgment in determining and aggregating internal control deficiencies, managers tend to attempt to persuade auditors for almost all control problems uncovered. Future research should more fully explore these explanations. For instance, control deficiencies defined as design deficiencies typically do not involve operational testing, and it is not clear whether management persuasion tactics would influence auditors differently for design versus operational control deficiencies. Additionally, very little is known about control deficiency aggregation and the effect of management explanation with respect to auditor judgment in such aggregation. Finally, future research should consider ways in which auditors can improve their assessments of internal control deficiency regardless of when and how management uses persuasion tactics.

REFERENCES

- Aerts, W. 2005. Picking up the pieces: impression management in the retrospective attributional framing of accounting outcomes. *Accounting Organizations and Society* 30 (6):493-517.
- Alicke, M. D. 2000. Culpable control and the psychology of blame. *Psychological Bulletin* 124 (4):556-574.
- Anderson, U., K. Kadous, and L. Koonce. 2004. The Role of Incentives to Manage Earnings and Quantification in Auditors' Evaluations of Management-Provided Information. *Auditing: A Journal of Practice and Theory* 23 (1):11-27.
- Arel, B., S. E. Kaplan, and E. O'Donnell. 2006. Halo effects during internal control evaluation: The influence of management self-assessment on auditor judgment. Working paper, Arizona State University.
- Ashbaugh-Skaife, H., D. Collins, and W. Kinney. 2005. The discovery and consequences of internal control deficiencies prior to SOX-mandated audits. Working paper. University of Iowa.
- Banham, R. 2006. Party of three: Outside advisors leap in where auditors fear to tread. *CFO* 22:56-64.
- Barton, J., and M. Mercer. 2005. To blame or not to blame: Analyst's reactions to external explanations for poor financial performance. *Journal of Accounting and Economics* 39:509-533.
- BDO Seidman LLP, Crowe Chizek and Company, Deloitte and Touche LLP, Ernst and Young LLP, Grant Thornton LLP, Harbinger PLC, KPMG LLP, McGladry and Pullen LLP, PricewaterhouseCoopers LLP, and W. F. Messier, Jr. 2004. A framework for evaluating control exceptions and deficiencies (Version 3). White paper.
- Bettman, J., and B. Weitz. 1986. Attributions in the board room: Causal reasoning in corporate annual reports. *Administrative Sciences Quarterly* 28:165-183.
- Bottom, W. P., K. Gibson, S. Daniels, and J. K. Murnighan. 2002. When talk is not cheap: Substantive penance and expressions of intent in rebuilding cooperation. *Organization Science* 13:497-513.
- Boury, P., and C. M. Spruce. 2005. Auditors at the gate: Section 404 of the Sarbanes-Oxley Act and the increased role of auditors in corporate governance. *International Journal of Disclosure and Governance* 2 (1):27-52.
- Crant, J. M., and T. S. Bateman. 1993. Assignment of credit and blame for performance outcomes. *Academy of Management Journal* 36 (1):7-27.
- Cullen, T. 2006. Nikon discloses breach of credit-card numbers. *The Wall Street Journal*:September 14, 2006.

- Earley, C. E., V. B. Hoffman, and J. R. Joe. 2006. The effect of management's classification of control deficiencies on auditor's judgments under PCAOB Auditing Standard Number 2. Working paper. Bentley College.
- Fields, G. 2006. Stolen disk leads to fears of VA privacy breach. *Wall Street Journal* May 23, 2006:A9.
- Gansler, J. S., and W. Lucyshyn. 2005. Improving the security of financial management systems: What are we to do? *Journal of Accounting and Public Policy* 24:1-9.
- Goffman, E. 1967. On face work. In *Interactin Ritual: Essays in Face-to-Face Behavior*, edited by E. Goffman. Chicago: Aldine.
- Hechinger, J. 2006. Fidelity employee left laptop with H-P data in car before theft. *The Wall Street Journal*:March 27, 2006.
- Heuberger, J. H., and B. J. Nepf. 2005. Taking control of internal control reporting: Recent PCAOB and SEC guidance. *Insights: The Corporate & Securities Law Advisor* 19 (7):2-9.
- IT Governance Institute (ITGI). 2005. *Control Objectives for Information and Related Technology 4.0 (COBIT)*. Rolling Meadows, IL: IT Governance Institute.
- Joyce, E. J., and G. C. Biddle. 1981. Anchoring and adjustment in probabilistic inferences in auditing. *Journal of Accounting Research* 19 (1):120-145.
- Kim, P. H., C. D. Cooper, D. L. Ferrin, and K. T. Dirks. 2004. Removing the shadow of suspicion: The effects of apology versus denial for repairing competence- versus integrity-based trust violations. *Journal of Applied Psychology* 89 (1):104-118.
- Kim, P. H., K. T. Dirks, C. D. Cooper, and D. L. Ferrin. 2006. When more blame is better than less: The implications of internal vs. external attributions for the repair of trust after a competence- vs. integrity-based trust violation. *Organizational Behavior and Human Decision Processes* 99 (1):49-65.
- Kline, R. B. 2005. *Principles and Practice of Structural Equation Modeling*. New York: Guilford Press.
- McQueen, M. P. 2006. Laptop lockdown. *Wall Street Journal* June 28, 2006:D1.
- Naquin, C. E., and T. R. Kurtzberg. 2004. Human reactions to technological failure: How accidents rooted in technology vs. human error influence judgments of organizational accountability. *Organizational Behavior and Human Decision Processes* 93:129-141.
- Nelson, M. W., J. A. Elliott, and R. L. Tarpley. 2002. Evidence from auditors about managers' and auditors' earnings management decisions. *The Accounting Review* 77 (Supplement):175-202.

- Ohbuchi, K., M. Kameda, and N. Agarie. 1989. Apology as aggression control: Its role in mediating appraisal of and response to harm. *Journal of Personality and Social Psychology* 56:219-227.
- Pacelle, M., and R. Sidel. 2005. Security is breached at card processor. *Wall Street Journal* June 20, 2005:A2.
- Public Company Auditing Oversight Board (PCAOB). 2004. *Auditing Standard Number 2 - An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*. Washington D.C.: PCAOB.
- Rapoport, M. 2005. Companies pay a price for security breaches. *Wall Street Journal* June 15, 2005:C3.
- Ricchiute, D. N. 1999. The effect of audit seniors' decisions on working paper documentation and on partners' decisions. *Accounting Organizations and Society* 24:155-171.
- Richmond, R. 2005. Who goes there? *Wall Street Journal* March 21, 2005:R11.
- Schonbach, P. 1990. *Account Episodes: The Management or Escalation of Conflict*. Cambridge, England: Cambridge University Press.
- Schwartz, G., T. Kane, J. Joseph, and J. T. Tedeschi. 1978. The effects of remorse on the reactions of a harm-doer. *British Journal of Social Psychology* 17:293-297.
- Shaw, J. C., E. Wild, and J. A. Colquitt. 2003. To justify or excuse?: A meta-analytic review of the effects of explanations. *Journal of Applied Psychology* 88 (3):444-458.
- Sidel, R. 2006. Credit firms to push to thwart fraud. *The Wall Street Journal*:September 25, 2006.
- Stata Press. 2005. *Stata Reference Manual*. College Station, TX: Stata Press.
- Tabachnick, B. G., and L. S. Fidell. 2000. *Computer-Assisted Research Design and Analysis*. Boston, MA: Allyn and Bacon.
- Tata, J. 2002. The influence of accounts on perceived social loafing in work teams. *The International Journal of Conflict Management* 13 (3):292-308.
- Weiner, B., J. Amirkhan, V. S. Folkes, and J. A. Verette. 1987. An attributional analysis of excuse giving: Studies of a naive theory of emotion. *Journal of Personality and Social Psychology* 52 (2):316-324.
- Wood, T. E., and T. R. Mitchell. 1981. Manager behavior in a social context: The impact of impression management on attribution and disciplinary actions. *Organizational Behavior and Human Performance* 28:356-378.
- Young, S. 2006. AT&T discloses online break-in. *The Wall Street Journal*:August 30, 2006.

TABLE 1
Profile of Participants' Experience and Assessment of Control Exceptions

Panel A: Experience

	<u>Number</u>	<u>Percent</u>
Number of Auditor Participants	106.00	100.00
Number of Auditor Participants With		
In-Charge Experience	92.00	86.79
In-Charge Experience SOX 404 Controls Audit	57.00	53.77
Involvement in SOX 404 Audit	92.00	86.79
Training on SOX 404	95.00	89.62
Training on AS 2	95.00	89.62
Auditor Participants Average	<u>Mean</u>	<u>Std. Dev.</u>
Months Of Audit Experience	37.62	19.78
Number of Clients with SOX 404 audits	1.52	1.03
Number of Clients with systems group interactions	2.16	1.25
Number of Clients with significant deficiencies	0.90	0.82
Number of Clients with material weaknesses	0.33	0.57

Panel B: Assessment of Control Exceptions^a

	<u>Mean</u>	<u>Std. Dev.</u>
Understood Control Exception ^b		
Case 1: Password Policy Violation - Invalid Sales Invoices	9.00	1.86
Case 2: Wrongly Granting System Access - Stolen Procurement Cards	8.68	1.73
Case 3: Unapproved Customer Credit	9.46	1.59
Case 4: Unrecorded Sales Discounts	9.13	1.84
Financial Statement Risk of Control Exception ^b		
Case 1: Password Policy Violation - Invalid Sales Invoices	7.93	2.42
Case 2: Wrongly Granting System Access - Stolen Procurement Cards	8.78	2.01
Case 3: Unapproved Customer Credit	8.50	1.94
Case 4: Unrecorded Sales Discounts	8.73	1.44

^a Each exception case was designed to be understandable, potentially have contributed to a more than inconsequential misstatement of the financial statements, and have its cause rooted in employee failure to follow procedures. Case 1 and case 2 represent the IT security breach condition. The first exception case involved placement of false sales orders using a password obtained from a stolen laptop where the employee had permanently stored their system password providing the mechanism for the exception. The second exception case involved a system access violation where the employee had provided access to an intruder who stole customer procurement card information. In the manual application control exceptions condition, the first exception case involved inappropriate credit approval overrides and the second exception case involved unrecorded discounts on sales. (See Appendix A for an excerpt of the experimental materials that describes the control exceptions.)

^b Assessments were made on 11-point scales with 11 representing high understandability and high consideration of financial statement risk.

TABLE 2
Management Blame for the Control Exceptions

Panel A: Means (Std. Dev.) Management Blame^a

<u>Control Exception Case</u>	<u>Control Exceptions</u>		<u>t-value</u>
	<u>IT Security Breach</u>	<u>Manual Application</u>	
Password Policy Violation vs. Unapproved Credit (IT Case 1 vs. Manual Case 3)	6.04 (2.56)	9.60 (1.49)	8.725*
Password Policy Violation vs. Unrecorded Discounts (IT Case 1 vs. Manual Case 4)	6.04 (2.56)	8.87 (1.77)	6.600*
Wrongly Granting System Access vs. Unapproved Credit (IT Case 2 vs. Manual Case 3)	8.07 (2.14)	9.60 (1.49)	4.245*
Wrongly Granting System Access vs. Unrecorded Discounts (IT Case 2 vs. Manual Case 4)	8.07 (2.14)	8.87 (1.77)	2.072**

Panel B: Repeated Measures ANOVA on Management Blame^b

<u>Source of Variation</u>	<u>SS</u>	<u>df</u>	<u>MS</u>	<u>F</u>	<u>p</u>
Between Subjects					
IT/Manual Control Exceptions	97.837	1	97.837	29.663	0.000
Concession/Denial	0.951	1	0.951	0.288	0.592
IT/Manual x Concession/Denial	0.143	1	0.143	0.043	0.835
Error	333.127	101	3.298		
Within Subjects					
Case	0.090	1	0.090	0.036	0.850
Case x IT/Manual Control Exceptions	23.439	1	23.439	9.443	0.003
Case x Concession/Denial	1.677	1	1.677	0.676	0.413
Case x IT/Manual x Concession/Denial	0.204	1	0.204	0.082	0.775
Error(case)	250.702	101	2.482		

*, ** Denotes significance at the 1% and 5% levels, respectively. Tests are two-tailed.

^a Management Blame = 11-point scale anchored by “no blame” and “all blame.”

^b The dependent variable for the repeated measures ANOVA equals the estimated error from the following regression: Management Blame = $\alpha + \beta_1(\text{effectiveness of compensating controls}) + \beta_2(\text{magnitude of misstatement}) + \beta_3(\text{likelihood of misstatement}) + \varepsilon$. Greenhouse-Geisser and Huynh-Feldt adjustment to degrees of freedom for sphericity violations validate the reported repeated measure results (Tabachnick and Fidell 2000). For sensitivity analysis, a repeated measures ANOVA that used management blame as the dependent variable was performed and it produced results identical to those reported above in terms of significant effects. Regressions using Huber-White corrected standard errors also produced results substantially identical to those reported above (Stata Press 2005).

TABLE 3
Descriptive Statistics - Mean (Std. Dev.) Auditor Perceptions and Judgments by Experimental Condition

Variables^a	IT Security Breach Control Exceptions						Manual Application Control Exceptions					
	Password Policy Violation			Wrongly Granting Access			Unapproved Credit			Unrecorded Discounts		
	Deny	Concede	t-value	Deny	Concede	t-value	Deny	Concede	t-value	Deny	Concede	t-value
	n = 27	n = 27		n = 26/27 ^b	n = 27		n = 24	n = 27/28 ^b		n = 24	n = 28	
Explanation Adequacy	4.22 (2.19)	6.22 (2.21)	3.343*	3.41 (2.10)	6.19 (2.48)	4.441*	3.79 (2.23)	4.26 (2.80)	0.655	3.58 (2.70)	3.14 (2.09)	0.663
Control Deficiency	7.30 (2.43)	5.74 (2.58)	2.280**	9.26 (1.72)	8.00 (2.63)	2.080**	8.58 (2.08)	8.54 (2.03)	0.083	8.13 (1.94)	8.43 (1.83)	0.579
Compensating Controls	-0.37 (2.04)	0.26 (1.99)	1.147	-1.48 (2.06)	-1.04 (1.93)	0.817	-1.63 (2.37)	-0.71 (1.88)	1.542	-0.96 (2.53)	-0.96 (1.75)	0.010
Magnitude of Misstatement	8.33 (2.59)	6.63 (2.93)	2.191**	9.23 (2.07)	8.04 (2.58)	1.856	7.92 (2.10)	8.14 (2.05)	0.392	7.79 (2.30)	7.68 (2.06)	0.187
Likelihood of Misstatement	7.26 (2.75)	6.96 (2.93)	0.383	8.30 (2.64)	7.11 (2.01)	1.856	8.13 (2.19)	7.68 (2.57)	0.668	8.29 (2.37)	8.04 (2.06)	0.458
Management Blame	6.44 (2.42)	5.63 (2.66)	1.176	8.33 (2.15)	7.81 (2.13)	0.890	9.54 (1.22)	9.64 (1.70)	0.243	9.00 (1.96)	8.75 (1.62)	0.504

*, ** Denotes significance at the 1% and 5% levels, respectively. Tests are two-tailed.

^a Control Deficiency = 11-point scale anchored by “no deficiency” and “significant deficiency”;
Explanation Adequacy = 11-point scale anchored by “not adequate” and “very adequate”;
Compensating Controls = 11-point scale anchored by “negatively influenced” and “positively influence”; scale ranged from -5 to 5;
Magnitude of Misstatement = 11-point scale anchored by “inconsequential” and “material”;
Likelihood of Misstatement = 11-point scale anchored by “remote” and “probable”;
Management Blame = 11-point scale anchored by “no blame” and “all blame.”

^b Cell sizes vary due to two missing responses: one in magnitude of misstatement and one in explanation adequacy.

Table 4
Repeated Measure ANOVAs for Perceived Explanation Adequacy and Control Deficiency Judgments

Panel A: Repeated Measures ANOVA on Perceived Explanation Adequacy^a

<i>Source of Variation</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>p</i>
Between Subjects					
IT/Manual Control Exceptions	87.834	1	87.834	10.554	0.002
Concession/Denial	78.074	1	78.074	9.381	0.003
IT/Manual x Concession/Denial	71.414	1	71.414	8.581	0.004
Error	840.590	101	8.323		
Within Subjects					
Case	14.395	1	14.395	5.138	0.026
Case x IT/Manual Control Exceptions	0.507	1	0.507	0.181	0.672
Case x Concession/Denial	0.008	1	0.008	0.003	0.956
Case x IT/Manual x Concession/Denial	8.446	1	8.446	3.015	0.086
Error(Case)	282.979	101	2.802		

Panel B: Repeated Measures ANOVA on Control Deficiency Judgments^a

<i>Source of Variation</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>p</i>
Between Subjects					
IT/Manual Control Exceptions	37.633	1	37.633	5.332	0.023
Concession/Denial	21.616	1	21.616	3.063	0.083
IT/Manual x Concession/Denial	31.130	1	31.130	4.411	0.038
Error	719.887	102	7.058		
Within Subjects					
Case	44.144	1	44.144	17.840	0.000
Case x IT/Manual Control Exceptions	75.373	1	75.373	30.582	0.000
Case x Concession/Denial	1.384	1	1.384	0.559	0.456
Case x IT/Manual x Concession/Denial	0.010	1	0.010	0.004	0.950
Error(Case)	252.393	102	2.474		

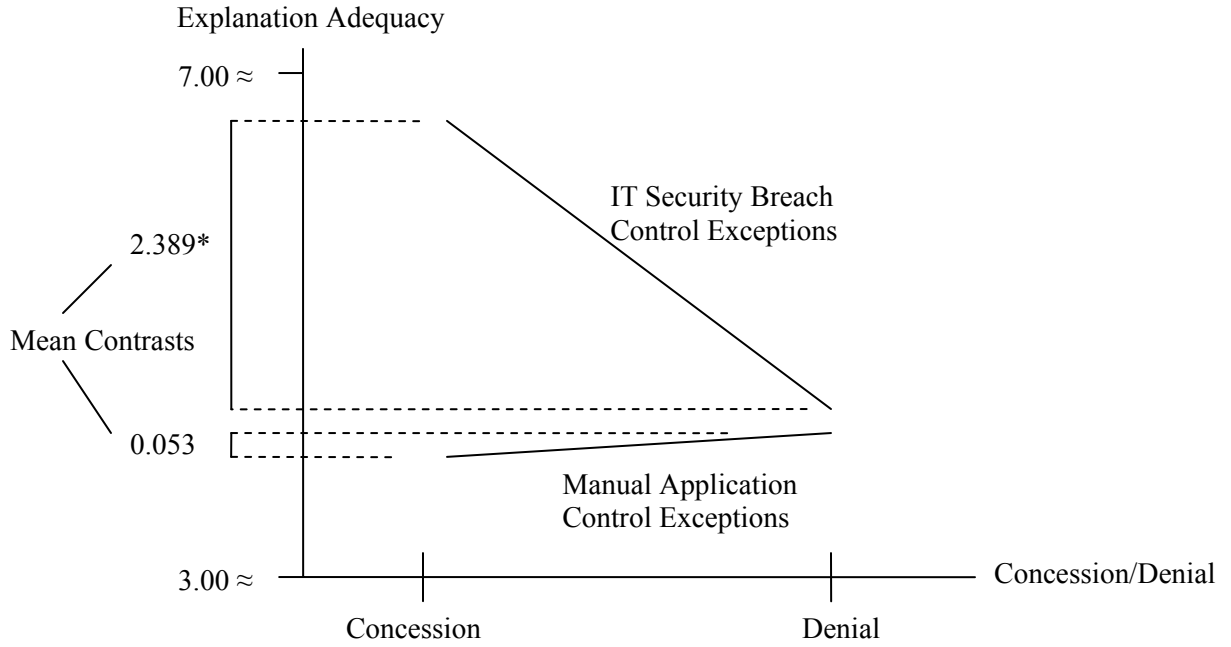
^a Greenhouse-Geisser and Huynh-Feldt adjustment to degrees of freedom for sphericity violations validate the reported repeated measure results (Tabachnick and Fidell 2000). For sensitivity analysis, regressions using Huber-White corrected standard errors were run and these produced results substantially identical to those reported above (Stata Press 2005).

Explanation Adequacy = 11-point scale anchored by “not adequate” and “very adequate”; Control Deficiency = 11-point scale anchored by “no deficiency” and “significant deficiency”

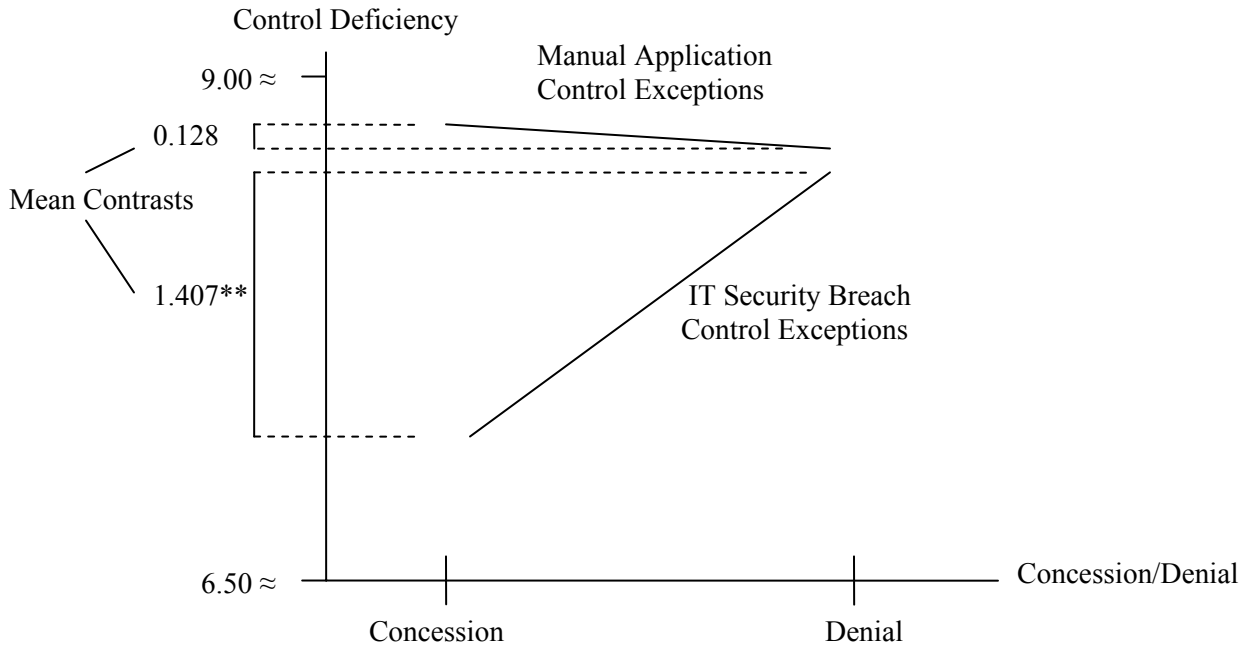
FIGURE 1

Graphs of the Interaction of IT Security Breach/Manual Application Control Exceptions and Concession/Denial for Perceived Explanation Adequacy and Control Deficiency Judgments

Panel A: Perceived Explanation Adequacy



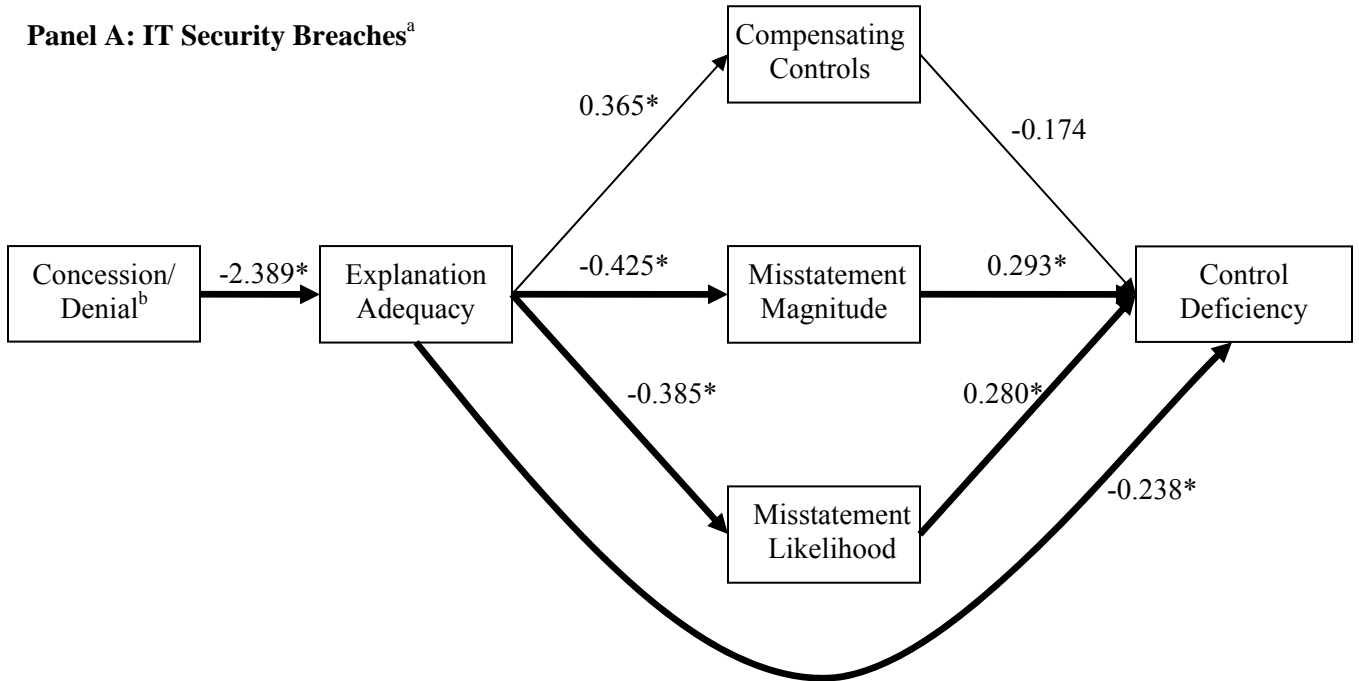
Panel B: Control Deficiency Judgments



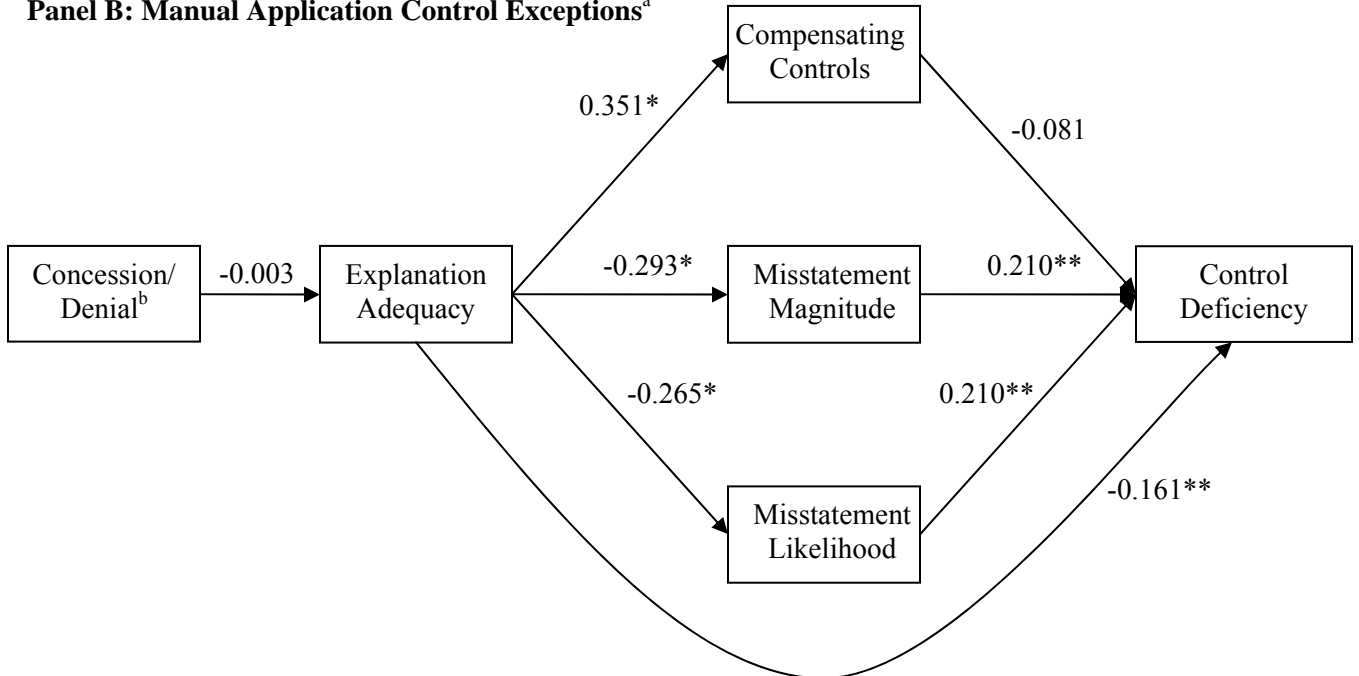
*, ** Denotes significance at the 1% and 5% levels, respectively. Tests are two-tailed.

Figure 2
Path Models of the Effect of Concession and Denial on Significance of Deficiency Judgments

Panel A: IT Security Breaches^a



Panel B: Manual Application Control Exceptions^a



*, ** Denotes significance at the 1% and 5% levels, respectively. Tests are two-tailed.

^a Modeled, but not shown, is a statistically significant, positive covariance between misstatement magnitude and likelihood judgments. (As shown in Appendix B, these judgments are highly correlated)

($\rho = 0.587$; $p < .001$). All alternative paths stemming from concession/denial were tested and were found statistically insignificant – explanation adequacy fully mediates the effects of concession/denial persuasion tactics under IT security breaches. Path models were estimated based on covariance matrices, and indicate good fit with the comparative fit index (CFI) $> .96$ and the standardized root mean square residual (SRMR) < 0.057 for both models (Kline 2005). Paths in bold indicate significant indirect effects stemming from concession/denial and are only found in the path model for IT security breaches. Indirect path parameter estimates and their t-values are as follows: 1) concession/denial => explanation adequacy => control deficiency (0.568, $t=2.481^{**}$); 2) concession/denial => explanation adequacy => magnitude of misstatement => control deficiency (0.297, $t=2.402^{**}$); and 3) concession/denial => explanation adequacy => likelihood of misstatement => control deficiency (0.258, $t=2.261^{**}$).

Appendix A
Experimental Materials: Internal Control Exceptions and Conversational Vignette

IT Security Breaches:

Specific Issues determined in testing information technology general controls:

1. A salesperson's laptop had been stolen. It contained a stored password that allowed a sales order to be downloaded to the system. Several bogus orders had been placed before the password was disabled.
2. Griffin's system had been breached in November. Indications are that approximately 2000 customer records were stolen from the customer master file. Much of the information lost was harmless. However, some of it would be of value to competitors. Additionally, approximately 500 of the customers had procurement card information on file.

IT Security Breaches Conversational Vignette:

The audit senior on the engagement, John, follows up on these issues with Derrick, the controller of Griffin Inc. The following is the discussion between John and Derrick.⁹

John: Hi Derrick. I scheduled this meeting with you to discuss some findings related to our controls audit. First, I'd like to discuss salesperson access to your sales order system.

Derrick: Sit down, John. I'd be happy to discuss that with you. Our salespeople work primarily from the field. So, we have provided them with laptops and that allows them to create sales orders and electronically file them from the field. Of course, both the laptops and our order entry system are password protected. What else can I tell you?

John: Well, I am familiar with the access controls that you just described; however, when we were performing our tests over information technology general controls, we reviewed password changes and found a cancelled password that we were told was due to a laptop theft. Apparently one of your salespeople lost their laptop and it contained the password for your order entry system?

Derrick: *John, I admit that we did have a small breach of controls in access. (John, this was not a control breach. This was an unusual incident due to circumstances beyond our control.)* The laptops themselves are password protected, but once that laptop is in the hands of a hacker, the laptop's password is almost useless. In this particular instance, our salesperson had permanently stored their system password on their laptop. So, once the thief had the laptop, they basically had access to our order entry system. Now, that said, as soon as the laptop was reported stolen, we disabled that password. Additionally, our credit manager reviews sales orders and if the order is to a new customer, he catches it. *John, I concede that we had a breach of a system access control, but as I said, our credit manager reviews sales orders. (John, people steal. We have controls that limit the damage from theft, but we cannot stop theft. This is not in our power. This is not a breach of controls.)*

John: Did any invalid sales orders get through?

⁹ Italicized text represents the concession manipulation. Italicized text in parenthesis represents the denial manipulation.

Derrick: Frankly, we did ship a very large order to one of our customers. Although they could have denied it, the order happened to be for product they normally carry so they accepted the order after they reported it. If those amounts hadn't been paid, that could have affected our results for this year. But, the important point is that the account was paid.

John: OK, let's get to the next issue. It appears that your main servers were hacked in November. Additionally, we found evidence that the customer master file was breached.

Derrick: *Again, John, I have to admit that security was breached. (Again, John, this was not a control breach. This system breach was due to circumstances beyond our control.)* It looks like we were socially engineered. Someone began attacking our system. Of course, our firewall picked it up. Then one of our system administrators got a phone call, and the caller said that our system was attacking his system. Our administrator said he didn't think that was the case and that we were being attacked also. In any event, the two decided that they would work on this problem together, and our administrator gave the caller access to part of our system. Well, the caller was the hacker and he used his access to our system to breach the customer master file. As you know, he got about 500 procurement card numbers. Luckily the liability on those is limited. *(John, how do you protect yourself against something like this? Bad guys are constantly trying to break into our system. We cannot control that. One of them just got through this time.)* And don't forget, John, we trained our people against this type of threat.

John: How quickly did you discover the breach?

Derrick: You know, John, that's the insidious thing. When one of our employees lets a hacker into our system, we don't have any mechanism to catch them. If we don't stop them at the gate, it's trouble. We didn't know that our system had been breached until the pro-cards started getting charged fraudulently, and it eventually led back to our shop.

John: Is there any possibility of an unrecorded liability here?

Derrick: No, I don't think so, John. It could have been larger, but we caught it in time. All the cards have been stopped. We've paid damages and none of our customers have indicated legal action. I think we are fine.

[pause as John considers the situation]

Derrick: Listen, John, we are very concerned that we maintain strong internal controls. *I readily concede that we had a couple of control issues. But, (We do not have issues with our controls. There is nothing wrong with our controls over system security. These issues that you've brought up are things that are beyond the control of any normal business or system. And,)* with our compensating controls, nothing has occurred that caused a material misstatement of profits.

Manual Application Control Breakdowns:

Specific Issues determined in testing application controls in the revenue cycle:

1. Near the end of the year, the electronic approval by the credit manager was missing for several customer orders that exceeded the credit limit. These orders were still processed without the approval.
2. The analysis of the daily unapplied cash exception reports indicated a number of unreported discounts to customers. Upon further investigation the auditor found that salespeople gave discounts to customers and failed to record them on the customer order. In most instances, adjustments to revenue were made without contacting the salespeople.

Manual Application Control Breakdowns Conversational Vignette:

The audit senior on the engagement, John, follows up on these issues with Derrick, the controller of Griffin Inc. The following is the discussion between John and Derrick.¹⁰

John: Hi Derrick. I scheduled this meeting with you to discuss some findings related to our controls audit. First, I'd like to discuss the controls over the approval of credit.

Derrick: Sit down, John. I'd be happy to discuss that with you. We have a credit manager who approves all customer credit limits and then approves all orders exceeding the credit limit specifically determined for each customer. When we have a new customer, our credit manager uses a software application that allows him to check credit ratings with three credit rating agencies. Once he has the credit ratings, he assigns a credit limit. He also reviews credit ratings for all customers on a semi-annual basis and adjusts the limits accordingly. For our largest clients, he performs this on a quarterly basis. When orders come in, they are checked against the current available credit limit. If there is not enough available credit, the order is reviewed. If approved, the credit manager uses a special password to approve the order and release it for processing. What else can I tell you?

John: Well, I am familiar with the process that you just described; however, when we were performing our tests over revenue cycle application controls, we found some orders that were missing an approval from the credit manager. It appears that these orders were routed through the system in another way and were filled without credit approval.

Derrick: *John, I admit that we did have a small breach of controls in credit approval. (John, this was not a control breach. This was an unusual incident due to circumstances beyond our control.)* During September, our credit manager was really sick and had to be out for several weeks. So, we performed a handful of system overrides to release orders for processing. *(We have no power over situations like this. The guy was so sick we couldn't even discuss the situation with him for over a week.)*

John: Oh. Who performed the override and did this individual check the available credit?

Derrick: The system override was performed by the Service Specialist Supervisor, Brenda. She was able to check available credit for our existing customers, but she could not access the software to check credit for new customers. *We would have liked to take the time to get the access, but we needed to process the*

¹⁰ Italicized text represents the concession manipulation. Italicized text in parenthesis represents the denial manipulation.

orders in a timely manner. It affected only a few new customers and we monitored it closely. John, I concede that we had a breach of this control, but as I said, we monitored it closely. (This was an isolated case based on events that were outside our control. It affected only a few new customers and we did not want to risk losing those customers simply because we couldn't check their credit in a timely fashion. We had no other alternatives and we monitored it closely. John, this is not a breach of controls.)

John: I guess the next question that I have is whether you know if this has had any impact on your financial statements.

Derrick: Frankly, we did have one new customer that placed a very large order that was approved without a credit check. If those amounts hadn't been paid, that could have affected our results for this year. But, the important point is that the account was paid.

John: OK, let's get to the next issue. It appears that customer discounts are not always recorded. Additionally, we found evidence that some unrecorded discounts are excessive.

Derrick: *Again, John, I have to admit that sometimes this control has been breached. (Again, John, this was not a control breach. This issue is due to circumstances beyond our control.)* Our salespeople are required to record all discounts and our system checks to ensure that discounts are within acceptable limits on all orders. But, the salespeople don't always do it. *(Sometimes, they get busy, forget and don't record the discount or get approval, but that's just human error outside our control. We remind them, but John, you know what salespeople are like. They're not like auditors. They just aren't as good about paperwork.)* However *(And)*, don't forget, John, I review a gross margin report on a monthly basis to make sure that something like excessive discounts doesn't get out of hand.

John: Is anyone doing anything else to ensure the accuracy of invoice amounts around quarter ends?

Derrick: No, because I am reviewing gross margin reports which would pick up any material misstatements. I fully recognize that our product line has wide variation in margins, but I think that I have enough experience to know if something is seriously out of whack.

[pause as John considers the situation]

Derrick: Listen, John, we are very concerned that we maintain strong internal controls. *I readily concede that we had a couple of control issues. But, (We do not have issues with our controls. There is nothing wrong with our controls over revenue. These issues that you've brought up are things that are beyond the control of any normal business or system. And,)* with our compensating controls, nothing has occurred that caused a material misstatement of profits.

Appendix B
Pearson Correlations (p-value)

	Control Deficiency	Explanation Adequacy	Compensating Controls	Magnitude of Misstatement	Likelihood of Misstatement	Management Blame
Control Deficiency	1					
Explanation Adequacy	-0.478 (0.000)*	1				
Compensating Controls	-0.363 (0.000)*	0.434 (0.000)*	1			
Magnitude of Misstatement	0.544 (0.000)*	-0.346 (0.000)*	-0.357 (0.000)*	1		
Likelihood of Misstatement	0.534 (0.000)*	-0.356 (0.000)*	-0.196 (0.004)*	0.587 (0.000)*	1	
Management Blame	0.591 (0.000)*	-0.416 (0.000)*	-0.392 (0.000)*	0.386 (0.000)*	0.422 (0.000)*	1

*, **, *** Denotes significance at the 1%, 5%, and 10% levels, respectively. Tests are two-tailed.

Control Deficiency = 11-point scale anchored by “no deficiency” and “significant deficiency”;

Explanation Adequacy = 11-point scale anchored by “not adequate” and “very adequate”;

Compensating Controls = 11-point scale anchored by “negatively influenced” and “positively influence”; scale ranged from -5 to 5;

Magnitude of Misstatement = 11-point scale anchored by “inconsequential” and “material”;

Likelihood of Misstatement = 11-point scale anchored by “remote” and “probable”;

Management Blame = 11-point scale anchored by “no blame” and “all blame.”