Impact of IS Governance Certifications on Enterprise Risk

Emergent Research Forum papers

Fernando Parra
University of Texas at El Paso
parra@utep.edu

Laura L. Hall, Ph.D.
University of Texas at El Paso
lhall@utep.edu

M. Adam Mahmood, Ph.D.
University of Texas at El Paso
mmahmood@utep.edu

Leopoldo Gemoets, D. Sc.
University of Texas at El Paso
lgemoets@utep.edu

Abstract

Business enterprises can seek external audits of their IS Governance controls in order to demonstrate that they are suitably designed and operating effectively in their supportive role of mitigating risk. SSAE 16-based SOC assurances and ISO 27001 certifications are third-party validations a business can obtain to increase stakeholder's trust on the organization's ability to safeguard its assets and operations. This study proposes to examine the impact of these certifications on enterprise risks as perceived by external investors of publicly traded companies in the U.S. A Risk-Adjusted Marked Model is proposed to examine market valuation effects, as measured by abnormal returns, as well as systematic risk effects, as measured by pre-event and post-event beta changes. For further insight, a cross sectional analysis relating risk changes to different types of certifications and firm characteristics is also proposed.

Keywords (Required)

ISO 27001, SSAE 16, IS Governance, ISMS value, ISMS risk effect, event study, beta-analysis

Introduction

Businesses all around the globe are increasingly concerned with the cyber risks that exist today given the advent of new technologies that are dependent on an interconnected world wide web. National efforts in the U.S. have aimed to monitor the increasing dependence on information technology through the enactment of legislative initiatives that create a partnerships between the public and private sector to protect enterprises. Among Post 9/11 U.S. government efforts to regulate information security policies, the most impactful legislations include the Federal Information Security Management Act (FISMA), establishing comprehensive information security requirements for the federal government and contractors, the Sarbanes-Oxley Act (SOX) Section 404, which provides a framework of control objectives for information technology, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which implement appropriate policies and procedures to comply with standards, implementation specification to protect patient privacy. As part of FISMA, the National Institute of Standards and Technology was made responsible for developing technology standards and compliance guidelines to safeguard information security. As a result, NIST developed a broad risk-management framework (RMF) that would serve as a vehicle for federal agencies to use in building information security into an organization’s infrastructure. NIST security standards and guidelines are developed through an open, public vetting process from both public and private stakeholders. While FISMA inducted the creation of key security standards and guidelines (FIPS 199 & 200, NIST publications 800-37, 800-53, 800-53a, 800-59 & 800-60), their efforts have expanded to address organizational issues, governance, and specific information asset protection.

Among such efforts, international standard ISO 27001 which specifies the requirements for “establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks” (ISO.org,
Impact of IS Governance Certifications on Enterprise Risk

2013). Such standard is suitable to be used by different types of organizations, and can be used by external as an auditing guide that lays out controls that an organization must address in order to obtain a certification of assurance. Similar to ISO 27001, other domain-specific assessment are offered and undertaken by certified authorities that create the standards and are licensed to execute the audit. SAS 70 Type II audits, now SSAE 16, by the American Institute of Certified Public Accountants, are designed to assess service auditor examinations, attestation reporting and information systems in a variety of service providers by globally accepted accounting principles (AICPA, 2013). Companies seeking this external audit are able to demonstrate to partners and customers that their organization's controls are in operation, suitably designed and operating effectively. This external validations is aimed at eliciting trust among partners, customers and stakeholders alike.

Research Purpose

IT governance, defined as “the process by which organizations seek to ensure that their investment in information technology facilitates strategic and tactical goals” (Debreceny 2013), is considered a subset of a broader corporate governance that is centered around IT’s role in an organization, particularly in the area of having appropriate organizational structures that promote the strategic alignment of organizational goals and IT outcomes, risk management, value and performance measurements (Wilkin and Chenhall 2010). A new stream of research has emerged investigating the various dimensions of information security governance in connection with third party assurances that aim to build trust with outside stakeholders of an organization. The integration of risk and information security management principles in IT governance that interconnect with other frameworks provides ample ground for research. Yet much is left to examine regarding the role of IT governance and risk management (Debreceny 2013). Despite the acknowledgements from organizations of the potential value of establishing information security standards such as ISO 27001, organizations may be reluctant to undertake such an enormous endeavor due to the costs associated with the benefits of implementations and the lack of knowledge of its cost/benefit ratio (Fenz et al. 2011). On the other hand, other studies provide evidence that assurances and third party security seals impacts the levels of trust on a company’s ability to safeguard data and information (Huang et al. 2011). As such, further steps should be taken to evaluate the validity in terms of risk mitigation value of such assurances.

This study aims to investigate and validate the impact of third party IS Governance certifications on enterprise risks as perceived by external investors. The following research questions are explored in this study:

- Does the external assurance of a company’s IS Governance result in an increase of market valuation for a publicly traded company?
- Does the external assurance of a company’s IS Governance result in a decrease of systematic risk for a publicly traded company?
- What firm characteristics moderate the impact of an IS Governance certification?
- Does the external assurance of a company’s IS Governance result in actual less reported internal control weaknesses for a publicly traded company?

Theoretical Framework and Hypotheses Development

The Resource-Based View (RBV) of the Firm (Barney 1991; Bharadwaj 2000) posits that firms derive competitive advantages from resources that are rare and valuable. This framework has provided a theoretical basis from which IS capabilities have been examined to explore competitive advantages (Chen et al. 2010). Thus, we draw from the RBV to analyze firm performance in terms of risk in comparison to the overall market to conduct this study. Financial economics provides a perspective of risk that can be conceptualized in two dimensions: systematic, which represents the risk associated with general market conditions, and unsystematic risk, which is unique and specific to a firm (Dewan & Ren, 2007). Using this perspective, unsystematic risk is perceived to be insignificant given the ability to diversify unsystematic risk away. The capital asset pricing model or CAPM (Treynor, 1962) provides a framework in which risk and return are positively related. The theory contends that all assets have a discount rate at which future cash flows produced by such assets should be discounted given the relative risk of the asset. CAPM makes certain assumptions about the investors (e.g. cost-free transactions, risk-averse investors and unlimited
investment capacities), and it asserts that all asset-specific risks can be paired by a beta index relative to the market beta of one. This perspective contends that systematic risk, measured by the sensitivity of the expected asset returns to the expected excess of market returns, cannot be mitigated. Thus, a measure of the success of enterprise risk management initiatives can be assessed by its reduction in its beta (Gordon et al., 2009). CAPM remains fairly popular given its simplicity and utility in a variety of scenarios despite its flaws when compared to more robust methodologies (Fama & French, 2004). Another theoretical basis of this study is the Market Efficiency Hypothesis, in which financial markets are presumed to be information-efficient. As such, investors cannot consistently achieve returns in excess of average market returns on a risk-adjusted basis, given the information available at the time the investment is made (Fama, 1970). This study presumes that information in the U.S. travels rather efficiently; thus, the potential effect of any public announcements made by publicly traded companies should be reflected in stock market reactions.

Although the financial view holds that firm-specific risk can be diversified away, strategic interventions such as IT investments can affect the risk/return profile of a firm (Otim et al., 2012; Tanriverdi & Rueflı, 2004). Given that enterprise systems affect several processes that are transformative to an organization, the timing of such investments in relation to the rest of the firms in an industry have been evidenced to downside reduce risk and provide strategic value in comparison to lower performing firms (Otim et al., 2012). The authors contend that this strategic management view of risk does in fact matter to a firm, even if it is firm-specific and often associated with unsystematic risk. However, if an event has affected the return of the security, there is no theoretical reason to believe that it has not affected the systematic risk of the security’s return. As such, this study adopts Dewan and Ren’s (2007)’s position and contends that if an investment event is so transformational for an organization, changes in systematic risk should be examined.

Based on the above discussion, Figure 1 depicts the hypothesized model:

**Figure 1. Proposed Research Model**

**P1:** Firms with public announcements of external IS Governance certifications will exhibit an increase of market valuation as measured by abnormal market returns.

**P2:** Firms with public announcements of external IS Governance certifications will exhibit a decrease in a company’s systematic risk.

**P3:** The systematic risk reaction of a firm that publicly announces an IS Governance certification will be moderated by the type of certification.
Methodology

The target sample of this study will be at least 100 U.S. publicly traded companies with public announcements of IS Governance certifications after the year 2002. To collect this sample, a search will be performed on the Lexis/Nexis Academic service and Google News. The search terms “implement”, “obtain”, “reach”, “certified” in conjunction with the terms “NYSE”, “AMEX”, “NASDAQ”, and “ISO 27001”, “COBIT”, “SSAE 16”, “SOC 1”, “SOC 2”. Subsequently, each press release will be inspected to verify corporation name, trading ticker, date of announcement, scope, venue, degree of implementation. Announcements within 30 days of each other will be consolidated to the first occurrence. Consistent with prior studies (Dewan et al. 2007), announcements will be eliminated if the Company has less than 120 days of trading history prior and after the events, no data exists at the Center for Research in Security Prices (CRSP), their average price in the estimation period was less than a $1, daily trading volume of less than 50,000 shares, or confounding announcements exist within a three-day window.

Risk-Adjusted Market Model Variables and Analysis

In order to jointly examine the effect of risk and return for the events, this study adopts a modified version of Dewan and Ren’s (2007)’s Risk-Adjusted Market Model as follows:

\[ R_{it} = \alpha_i + \alpha'_i D_t + \beta_i R_{mt} + \beta'_i D_t R_{mt} + \beta_i R_{mt} + \epsilon_{it} \]  (1)

Under this model, \( R_{it} \) represents stock returns on the market portfolio \( R_{mt} \). The dummy variable \( D_t \) represents the pre (value 0) and post event (value 1) window, providing an opportunity to measure the parameters \( \alpha_i \) and \( \beta'_i \) to measure the value of alpha and beta respectively. The analysis uses 120 trading days to calculate the pre-event and post-event estimation window to allow the segregation of return and risk effects. The event window is conducted based on \( t, t+1 \) trading days. Since both risk and return are considered to be closely correlated, heteroscedasticity may be suspected. As such, an OLS regression with robust standard errors that estimates the asymptomatic covariance matrix of the estimates is a more adequate methodology to address normality, heteroscedasticity and large residual concerns (White 1980). The model is applied to the data set for each firm in order to obtain parameter estimates. Once the model contained in equation 1 is applied to all the firms, the resulting coefficients \( \alpha_i \) and \( \beta_i R_{mt} \) along with the actual realized return \( R_{it} \) is used to calculate the corresponding abnormal returns (\( AR_{it} \)), or the deviation of realized returns from the expected returns, for each firm. Equation 2 depicts the calculation of abnormal returns:

\[ AR_{it} = R_{it} - (\alpha_i + \beta_i R_{mt}) \]  (2)

For purposes of this study, the cumulative abnormal return (\( CAR_i \)) variable for firm \( i \) is calculated by summing the abnormal returns for the 3-day event window containing the announcement day plus and minus 1 day (-1,0,1). This variable is subsequently aggregated as an average (\( CÅR \)) across all firms or across firms within subgroups (e.g. firms that obtained new certification versus renewals) as depicted in Equation 3:

\[ CÅR = \frac{1}{N} \sum_{i=1}^{N} CAR_i \]  (3)

To provide further insight into the results, a cross sectional analysis relating risk changes to various event and firm characteristics is conducted. This analysis will examine the determinants of total risk as depicted in Equation 4:

\[
\DeltaSysRisk_{it} = \alpha_0 + \alpha_1 PreSysRisk_{it} + \alpha_2 Ret_{it} + \alpha_3 New_{it} + \alpha_4 ISO_{it} \\
+ \alpha_5 SOC1_{it} + \alpha_6 SOC2_{it} + \alpha_7 FirmSize_{it} + \epsilon_{it}
\]  (4)
Where for each company $i$ at time $t$: “PreSysRisk” represents the systematic risk that existed in the estimation period prior to the event as calculated by Equation 1. “Ret” represents the average return over the prior 120 days, included given the hypothesis that returns are associated with risk. “New” represents a dummy variable of 1 for a new assurance certification or 0 for an updated one. “ISO” represents a dummy variable coded with 1 for ISO-27001 certification. “SOC1” represents a dummy variable coded with 1 for SOC 1 assurance statements obtained based on SAS 70 or SSAE 16 standards type I or II. Similarly, “SOC2” represents a dummy variable coded with 1 for SOC 2 assurance statements. Finally, previous literature suggests that certain firm characteristics may influence a company’s overall risk (Bharadwaj et al. 1999; Chen and Lee 1993; Dewan et al. 2007; Otim et al. 2012); For control variables, FirmSize is operationalized as the logarithm of market value of the firm on the event day.

Conclusion

IS Governance aims to provide an organization with a coherent set of policies, processes and systems to manage information asset risks, ensuring acceptable levels of information security risk. As such, the certification of such efforts would signal external stakeholders that internal controls exist in a company. Given the extraneous efforts a company must follow, this study offers a quantifiable method to assess the effect on a company’s valuation, its systematic risk effects, and the certification and firm characteristics that may affect those effects. This study answers researchers’ call to evaluate the validity in terms of risk mitigation value of such assurances. Practitioners would benefit from confirming the value of undertaking a non-mandated assurance by third party, motivating companies to adopt ISMS that can help reduce future security incidents.

REFERENCES


Impact of IS Governance Certifications on Enterprise Risk