Impact of Enterprise System Implementations on Enterprise Risk

**Abstract**

The use of sophisticated enterprise systems compels changes in underlying business processes, leading to reengineering efficiency improvements that are normally compounded by the benefits of automation; enterprise systems implementations, however, can also represent unique risk issues. This study proposes to examine the impact of enterprise system implementation 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 enterprise systems and firm characteristics is also proposed.

**Keywords**

Enterprise Systems, ERPs, ERP value, ERP risk effect, event study, beta-analysis

**Introduction**

Today’s business environment is complex, volatile, and exposed to substantial global risks that consistently affect the day-to-day operations and decision making process of any organization. Given the increasing complexity of most markets, in addition to the increasing dependence on digital information, risk mitigation can no longer be bound to uncoordinated efforts surrounding core business functions limited to compliance, internal controls, audits and incident response. Isolated compliance, valid internal controls and risk-transfer practices can no longer protect an enterprise from today’s real market risks. Instead, businesses must transform traditional procedures into strategic, enterprise-wide, risk management methodologies that identify, manage and minimize risks in order to ensure business success and continuity.

Enterprise systems are integrated software packages that automate core business functions such as finance, human resources, and logistics. Organizations normally implement enterprise systems to integrate their data flows and improve their business operations, including supply chain management, inventory control, manufacturing scheduling and production, sales support, customer relationship management, financial and cost accounting, human resources, and almost any other data-oriented management process (Hitt et al. 2002). In addition, enterprise systems can optimize the control of identity and access management. Industrial and professional reports often claim that the basic drivers motivating the adoption of enterprise systems include: cost reduction, improved efficiency, reduced product cycle time, improved customer service and satisfaction, the ability to change and configure business in response to changing market, and enabling e-commerce. Enterprise system adoptions are normally motivated by better regulatory compliance, business process reengineering, integration of operations and management decision support (Robey et al. 2002). Such adoptions may also be driven by the goals of creating lasting shareholder value and safeguarding the organization from the consequences of information system disasters (Debreceny 2013; Parent and Reich 2009).
The use of such sophisticated enterprise systems compels changes in the underlying processing, leading to reengineering efficiency improvements that are normally compounded by the benefits of automation; enterprise systems implementations, however, can also represent unique risk issues. As organizations integrate their data flows and improve their business operations and decision making process, organizations face a unique set of new risk components derived from the tightly-linked interdependencies of business processes (M.-K. Chang et al. 2008) and the possibility of implementation failure (Ngai et al. 2008). On the other hand, it also presents a distinctive opportunity for the integration of enterprise-wide risk management efforts that support internal control processes (Debreceny 2013; Parent and Reich 2009; Wright and Wright 2002). Key enterprise systems characteristics that impact security and internal controls include degree of standardization, centralization, authorization, and access to functions, as well as, automation of controls versus existing internal control structure (Scapens and Jazayeri 2003). Earlier studies suggest that enterprise systems impact an organization’s management control systems by increasing the centralization of system coordination and homogenization of control practices (Granlund and Malmi 2002; Kallunki et al. 2011); and, it is further suggested that firms that have implemented enterprise systems are less likely to report internal control weaknesses than those firms without such enterprise technology (Morris 2011). Based on the well-established premise that enterprise systems can provide organizations with competitive advantages through improved operational, tactic and strategic business performance (Chand et al. 2005; Dehning et al. 2007; Gefen 2005; Häkkinen and Hilmola 2008; Hayes et al. 2001; Hunton et al. 2003; Nicolau 2004; Nicolaou and Bhattacharya 2006), publicly-traded company investors have been evidenced to react positively to enterprise system implementation announcements (Hayes et al. 2001; Hendricks et al. 2007; Hitt et al. 2002; Wier et al. 2007). Furthermore, the market has been demonstrated to react to firms with ES investments upon full implementation, reflecting an inherent stock discount due to the existence of substantial enterprise risks that are eventually outperformed by the benefits of this technology (Hitt et al. 2002). More than a decade of transformative software development in enterprise systems has occurred since these studies took place, including the integration of business intelligence, cloud-based services, API interconnectivity, auditing modules and government regulatory compliance component tools. In addition, over the last decade, U.S. legislative changes have significantly increased the disclosure requirements regarding publicly-traded companies’ internal material weaknesses, providing a significant factor in a company’s market-adjusted cost of equity and information risks (Ashbaugh-Skaife et al. 2009). Such new tools, combined with a history of implementation lessons learned and new disclosure requirements may alter the authority of previous research findings.

**Research Purpose**

Given the cited dialogue in the literature surrounding the impact of enterprise system implementations on risk mitigation in addition to this decade’s technology and regulatory developments, this study aims to examine enterprise risk net-effects caused by the changes in the interdependencies in business process and internal controls caused by such implementations. This study proposes to examine the impact of enterprise system implementation 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 enterprise systems and firm characteristics is also proposed.

**Enterprise Systems, Internal Controls and Risk**

The auditing community has established three different categories of risks: business interruption risks, which refer to the likelihood that endogenous or exogenous factors will disrupt a company’s ability to timely process transactions, process interdependency risks, which refer to those risks arising from the transit of information from one process to another; and system security risks, which are based on the organizational behavior or external mischief (Hunt et al., 2004) and can be further segmented into the classical CIA Framework (ISO/IEC 2013). While business interruption risks are considered to be inherent to any business, both process interdependency and system security risks are considered risks that can be controlled with policies, procedures and information tools that may mitigate their damage.
A holistic approach toward managing such organization’s risk, commonly known as enterprise risk management (ERM), is suggested to improve an organization’s performance contingent upon the appropriate match with its contextual variables specific to each organization (Gordon et al. 2009). Authors suggest ERM efforts benefit firms by decreasing volatility in earnings and stock prices, decreasing external capital costs and increasing capital efficiency (Gordon et al. 2009; Hoyt and Liebenberg 2011; Nocco and Stulz 2006). As enterprise systems continue to interlace with broader, enterprise-wide operations, decision management and internal controls, they often interact and impact an organization’s ERM efforts. These systems share data across functional divisions and hierarchy levels which can be turned into valuable information for an organization’s decision making, intelligence and risk management capability goals. As such, the operational uncertainties derived from non-standard processes and lack of access on a real-time basis to relevant information can be minimized by the proper data exploitation strategies (Mathrani and Mathrani 2013). Enterprise systems can thus be critical to improve the organization’s knowledge and its ability to make more informed decisions (Grabski et al. 2011). The very same nature of enterprise systems that may systematically align them to monitor and mitigate risks at an enterprise level, also makes them unique to challenges beyond the scope of project failure, that rise from the integration of external consultants, simultaneous integration and reengineering of processes (Grabski et al. 2011; Somers et al. 2001). The interdependency of business processes may very well heighten the potential risk of financial misstatements and defalcations (Wright and Wright 2002).

A scholarly focus has recently emerged on examining the impact of enterprise systems on organizational controls and risks that go beyond the scope of assessing potential implementation failures and critical success factors with mixed results. Enterprise systems are posited to permit the standardized control of user knowledge, role and system privileges, improving information quality (Häkkinen and Hilmola 2008), management controls (Chapman and Kihn 2009; Elmes et al. 2005; Kallunki et al. 2011), accessibility to continuous auditing (S.-I. Chang et al. 2008; Kuhn Jr. and Sutton 2010) and financial reporting controls (Mundy and Owen 2013). However, opposing evidence also suggests that enterprise systems do not materialize in more effective internal controls (Granlund and Malmi 2002), even suggesting that the increased forecasting capacity from the systems may lead to manipulation of earnings forecast disclosures (Brazel and Dang 2008). O’Leary (2000) suggests that the degree of improved management controls may be attributed to whether a system is initially configured to provide such benefits, citing the circumvention and override of controls often due to implementation timeline demands. As such, enterprise systems may allow the unfettered access to information and processes if controls are not set in place (Grabski et al. 2011).

Regulatory requirements that compel companies to reduce enterprise risk by providing stronger internal controls and information systems security (e.g. Sabanes-Oxley Act, Health Insurance Portability and Accountability Act) have opened an opportunity for vendors to respond with enhanced audit modules and continuous audit support. Notable trends in risk management and regulatory research explore the role that enterprise systems play in reducing risk by supporting compliance (Grabski et al. 2011; Maurizio et al. 2007; Mundy and Owen 2013). Multinational corporations are subjected to an expanded set of regulations, making this area of research even more relevant. Nonetheless, security risks continue to be prevalent due to the interconnectivity, integration, and automation of business processes, whereby a single user may be able to trigger enterprise-wide reactions in both data and processes (Ko Hsu et al. 2006). In addition to control elements that affect enterprise risks, such as centralization, authorization levels, automation of controls (Hunton et al. 2004; Scapens and Jazayeri 2003), studies have shown enterprise systems can provide managers with the ability to manipulate reported performance by using smaller magnitude adjustments in cases of impending shortfalls unless significant internal controls are instituted (Stratopoulos et al. 2013), increase the potential for control weaknesses (Wright and Wright 2002) or fail to provide separation of duties if inappropriately configured (McCollum et al. 2003). In comparing risk assessments performed by IT auditors versus financial auditors, Hunton and colleagues (Hunton et al. 2004) suggest that both auditors “indicate significantly higher business interruption, process interdependency and overall control risks” (p. 7) with enterprise systems in comparison to legacy systems; and, IT auditors recognize significantly higher network, database and application security risks while financial auditors do not, suggesting that financial auditors may fail to adequately assess the appropriate degree of risk of those companies using enterprise systems.

Yet, other studies strongly suggest that enterprise systems change an organization generating knowledge-leveraging actions at both executive and operational levels that reduce operational risks (Mathrani and
Mathrani 2013). After controlling for variables that usually contribute to internal control weaknesses, Morris (2011) suggests firms are less likely to report material weaknesses after implementing an enterprise system. Dorantes et alia (2013) suggest that enterprise systems can provide managers with enhanced accuracy of management earnings forecasts based on better access to decision-relevant internal information. Even if a previous study can be used to manipulate earnings reports (Braziel and Dang 2008), others studies find contradictory evidence in that regard (Dorantes et al. 2013; Morris and Laksmana 2010). Studies also suggest that the cited risks associated with enterprise systems exhibited across life cycles are predominantly manifested only in those organizations that exhibit issues during the early stages of implementation, citing lack of organizational readiness (Aloini et al. 2007). Combined with formal management controls, enterprise systems have also been evidenced to improve firm performance and reduce risks (Kallunki et al. 2011).

Furthermore, enterprise system vendors have also evolved tremendously in the last decade, providing additional access control, compliance auditing and risk management modules that respond to their clients’ evolving security and regulatory compliance needs (Grabski et al. 2011). In addition to evidentiary support of risk mitigation, compliance and internal control benefits, the literature is abundant with support of operational (Cotteleeer and Bendoly 2006; Dehning et al. 2007; Hunton et al. 2003; Madapusi and D'Souza 2012; Poston and Grabski 2001; Su and Yang 2010), tactical (Bose et al. 2008; Dehning et al. 2007; Madapusi and D'Souza 2012; Su and Yang 2010), strategic (Chand et al. 2005; Su and Yang 2010) and financial performance benefits (Hendricks et al. 2007; Hunton et al. 2003; Nicolaou 2004; Wier et al. 2007).

Although both internal and external methods have been offered by the literature to evaluate the value of technology, studies suggest that the relationship between technology investment and financial performance is “marginally, but significantly, stronger in studies that employ market measures rather than accounting measures of financial performance” (Lim, Dehning, Richardson, & Smith, 2011). Thus, the evaluation of perceived risks by market measures would be a viable measurement of a company’s risk status. To this effect, studies have shown stock market reaction to implementations of enterprise systems with mixed results (Hayes et al. 2001; Hendricks et al. 2007; Roztocki and Weistroffer 2009; Rubin and Rubin 2013). While other effects of IT investments on stock prices have been intensively researched, studies on the effects of IT investments on volatility have only recently emerged. For the exception of Rubin and Rubin (2013)’s study, these studies have focused mainly on abnormal stock returns, not financial risk. Furthermore, as suggested by Dewan and Ren (2007), these studies are based on a consistent risk level and ignore the compounding risk effects of the event itself by not jointly examining both wealth and risk impacts that affect the market in the same direction and cannot be separated absent of explicit controls for risk effects. Dewan and colleagues evidence that abnormal returns are associated with IT by incorporating IT risk measures (Dewan et al. 2007). Tanriverdi and Ruefli (2004) further support this notion and observe that

“Studies that examine the business value of IT only from the return perspective are overlooking risk/return tradeoffs. Incorporating risk into the analysis is critical for developing a more complete understanding of the performance effects of IT. At a minimum, studies focusing on the return implications of IT should control for associated risks.” (Tanriverdi and Ruefli 2004, p. 441)

As such, an event study methodology that “extends the estimation window to include both pre-event and post-event data and allows for the market model parameters α and β to change following the event” (Dewan and Ren 2007, p. 374) would provide further insight.

Given this ongoing scholarly discussion regarding the impact of enterprise systems on organizational value and risk in addition to the evolving capabilities of enterprise systems since most studies took place, this study aims to answer Otim et alia’s (2012) call to examine the impact of investments in enterprise technology on risk, as perceived by external stakeholders by adopting a methodology that may improve on previous opportunities.

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. As exemplified by the literature review,
Impact of Enterprise System Implementations on Enterprise Risk

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 and 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. 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). 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). Under this premise, investors anticipate results from initiatives that may take several months to either implement or derive a benefit and react to that investment in today’s time.

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 (Otím et al. 2012; Tanriverdi and Ruefli 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 (Otím 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 and unsystematic 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.

Figure 1 depicts the proposed model for this study, based on Dewan and Ren’s (2007)’s Risk-Adjusted Market Model.

**Figure 1. Proposed Research Model**

*Value of enterprise system implementations and updates*

As summarized in previous sections, there is an extensive stream of literature that has investigated the impact of information technology investments on an organization’s financial and non-financial performance (e.g. Bharadwaj, 2000; Brynjolfsson & Hitt, 2003; Dehning et al., 2007; Kohli & Devaraj,
2003; Otim et al., 2012). Specific enterprise system implementation research have validated the valuable impact of these systems in spite of all cited costs and risks associated with these enterprise implementations (Grabski et al. 2011). Operational benefits are evidenced to include higher operational knowledge and more efficient inventory turnover, production flow, order lead times, processing times, as well as, reduced cost of goods sold, inventory turnover and availability of products (e.g. Baskerville, Pawlowski, & McLean, 2000; Bose, Pal, & Ye, 2008; Cotteleer & Bendoly, 2006; Dehning, Richardson, & Zmud, 2007; Gefen, 2005; Madapusi & D’Souza, 2012; Poston & Grabski, 2001). Tactical benefits include significant improvements in customer vendor collaboration, decision making, scheduling, quality management, change management, process management, resource planning, transparency and organizational standardization (e.g. Becker, Greve, & Albers, 2009; Bose et al., 2008; Chand et al., 2005; Cotteleer & Bendoly, 2006; Gefen, 2005; Häkkinen & Hilmola, 2008; Madapusi & D’Souza, 2012). Strategic benefits cited include market growth, capitalization, new markets, better forecasting, as well as higher competitive advantages in return-on-assets, return on investments (e.g. Chand, Hachey, Hunton, Owhoso, & Vasudevan, 2005; Dehning, Richardson, & Zmud, 2007; Hayes, Hunton, & Reck, 2001; Hendricks, Singhal, & Stratman, 2007; Hitt, Wu, & Xiao Zhou, 2002; Nicolaou & Bhattacharya, 2006; Nicolaou, 2004; Su & Yang, 2010). Thus, the following hypothesis is proposed:

**P1:** Firms with public announcements of enterprise system implementations will exhibit an increase of market valuation as measured by abnormal market returns.

### Risk Effect of enterprise system implementations and updates

As summarized previously, enterprise systems have been evidenced to provide better internal control that are derived from data processing integration, access and security centralization, and system usage standardization (Sia et al. 2002), permitting the standardized control of user knowledge, role and system privileges, improving information quality (Häkkinen and Hilmola 2008). When configured appropriately, they can support management control (Chapman and Kihn 2009; Elmes et al. 2005; Kallunki et al. 2011) auditing (S.-I. Chang et al. 2008; Kuhn Jr. and Sutton 2010), and compliance purposes (Grabski et al. 2011; Maurizio et al. 2007; Mundy and Owen 2013). Although dissenting literature disputes the ability to materialize such benefits (Brazel and Dang 2008; Granlund and Malmi 2002), enterprise systems have also been evidenced to improve firm performance and reduce risks (Kallunki et al. 2011). The literature also suggests that enterprise systems can serve as management control system packages integrating various accounting and non-accounting control systems (Granlund 2009). Given that enterprise systems have been evidenced to be a part of enterprise-wide risk management efforts that can decrease volatility in earnings and stock prices, decreasing external capital costs and increasing capital efficiency (Gordon et al. 2009; Hoyt and Liebenberg 2011; Nocco and Stulz 2006), the financial economics would offer support to examine the impact of enterprise systems on systematic risk. Thus, the following hypotheses are offered:

**P2:** Firms with public announcements of enterprise system implementations will exhibit a decrease in a company’s systematic risk.

Given the magnitude of enterprise system implementation, a myriad of challenges (e.g. insufficient technical expertise, organizational fit factors, project management issues) have been historically found to impact the overall success of a new risk ERP implementation (Sumner 2000). Organizations, however, tend to acquire resources with time and overcome learning challenges. Furthermore, studies have differentiated the value obtained from initial implementations from subsequent upgrades and updates suggesting that enhancements that occur within a few years of the post-implementation may signify that the system is well adopted and that any additional initiatives serve strategic purposes (Nicolaou and Bhattacharya 2006; Otim et al. 2012; Roztocki and Weistroffer 2009). While this study posits that implementation of enterprise systems will reduce the systematic risk in a firm, such reduction should be affected by the history of enterprise system implementations by that firm. Thus, the following hypothesis is offered:

**P3:** A firm’s systematic risk reduction exhibited after a public announcement of an enterprise system will be affected by whether the firm is engaging in a new project or an update to an already existing system.

Studies suggest that investors may discern the purpose of system implementations at the time of the announcement and react differently if such purpose is meant to serve transformational, strategic and
innovative purposes for an organization, as opposed to automation purposes (Otim et al. 2012; Dos Santos et al. 1993). During the last decade, vendors have transformed their enterprise systems to include modules that go beyond the integration of business functions; such capacities include, but are not limited to, business intelligence, compliance and risk management (Grabski et al. 2011; Mathrani and Mathrani 2013; Rubin and Rubin 2013). In addition to these enhancements, vendors have emerged with cloud-based and hybrid systems that offer on-demand, scalable enterprise software online. SAP Business ByDesign and Sage 300 ERP Online are a few examples of these platforms. The purpose of system implementations at the time of the announcement, the development of more sophisticated software capacities into support an organization, and the availability of cloud-based infrastructure may cause moderating effects on risk interactions. Thus, the following hypotheses are offered:

**P4:** A firm's systematic risk reduction exhibited after a public announcement of an enterprise system will be affected by whether the firm is implementing a cloud-based system.

**P5:** A firm's systematic risk reduction exhibited after a public announcement of an enterprise system will be affected by whether the firm is implementing a system that includes a business intelligence module.

**P6:** A firm's systematic risk reduction exhibited after a public announcement of an enterprise system will be affected by whether the firm is implementing a system that includes a government regulatory compliance module.

### Methodology

The target sample of this study should contain at least 100 U.S. publicly traded companies announcing an upgrade or implementation of an enterprise systems on or after the year 2002. To collect this sample, a search is performed on Lexis/Nexis and Google News with relevant key terms. Announcements within 30 days of each other are consolidated to the first occurrence. Consistent with prior studies (Dewan et al. 2007), announcements are eliminated if the company has less than 120 days of trading history prior and after the events, no data existed at the Center for Research in Security Prices (CRSP) or confounding announcements within a three-day window.

### Risk-Adjusted Market Model and Analysis

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

\[ R_{it} = \alpha_i + \alpha' D_t + \beta_i R_{mt} + \beta_i D_t R_{mt} + \epsilon_{it} \]  

(1)

Under this model, Rit represents stock returns on the market portfolio Rmt. The dummy variable Dt represents the pre (value 0) and post event (value 1) window, providing an opportunity to measure the parameters \( \alpha' \) and \( \beta' \) 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 \( R_{it} \) are used to calculate the corresponding abnormal returns (ARi), 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 (CARi) 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 (C\( \bar{A} \)R) across all firms or
across firms within subgroups (e.g. firms that implemented new systems versus updates) as depicted in Equation 3:

\[
C\bar{A}R = \frac{1}{N} \sum_{i=1}^{N} CAR_i
\]  

(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:

\[
\Delta SysRisk_{it} = \alpha_0 + \alpha_1 PreSysRisk_{it} + \alpha_2 Ret_{it} + \alpha_3 New_{it} + \alpha_4 BI_{it} + \alpha_5 Cloud_{it} + \alpha_6 GRC_{it} + \\
\alpha_7 FirmSize_{it} + \alpha_8 Leverage_{it} + \alpha_9 NewCloud_{it} + \alpha_{10} NewBI_{it} + \epsilon_{it}
\]  

(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 system implementation or 0 for an update to an existing system. “Cloud” represents a dummy variable coded with 1 for cloud-based systems and 0 for traditionally in-house systems. “GRC” represents a dummy variable coded with 1 for systems containing government regulatory compliance modules and 0 without such modules. Similarly, “BI” represents a dummy variable coded with 1 for systems containing business intelligence modules and 0 without them. “NewCloud” represents a dummy coded 1 for the implementation of new cloud systems, and “NewBI” for the implementation of new business intelligence systems, as opposed to updates of the same. 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, Leverage is included as the ratio of total long term divided by the total assets of the company during the event’s fiscal year; and FirmSize, operationalized as the logarithm of market value of the firm on the event day.

**Conclusion**

While enterprise systems have been posited to provide unique risks due to their massive organizational impacts, they also have been posited to transform an organization’s strategic position, its governance and its culture. This study aims to answer the call to examine the impact of investments in enterprise technology on risk, as perceived by external investors (Otim et al., 2012). The methodology offered updates and supplements on previous invaluable contributions in the literature, by jointly analyzing abnormal returns and systematic risk effects of enterprise system implementations and updates. Moderating effects of the main purpose of the enterprise system, its infrastructure, and other components is a relevant discussion given the last decade advances in technology that include cloud services. Additionally, as other large and medium-sized firms select enterprise systems as their primary information systems, this study will highlight the practical security risks improvements made by their investments.

**REFERENCES**


