2009

Disintegrating Information Technology in Corporate Divestures: Implications for Regulatory Compliance Risks and Costs

Huseyin Tanriverdi
University of Texas at Austin, huseyin.tanriverdi@mccombs.utexas.edu

Kui Du
University of Texas at Austin, kui.du@phd.mccombs.utexas.edu

DISINTEGRATING INFORMATION TECHNOLOGY IN CORPORATE DIVESTITURES: IMPLICATIONS FOR REGULATORY COMPLIANCE RISKS AND COSTS

Completed Research Paper

Hüseyin Tanriverdi
The University of Texas at Austin
Red McCombs School of Business
Department of Information, Risk, and Operations Management
CBA 5.202 B6500, Austin, TX 78712
E-mail:
Huseyin.Tanriverdi@mccombs.utexas.edu

Kui Du
The University of Texas at Austin
Red McCombs School of Business
Department of Information, Risk, and Operations Management
CBA 5.202 B6500, Austin, TX 78712
E-mail:
kui.du@phd.mccombs.utexas.edu

Abstract

Prior research has paid very little attention, if at all, to the risks and costs entailed in IT disintegration processes. In this study, we begin addressing this gap by studying how IT disintegration challenges posed by corporate divestitures affect the regulatory compliance risks and costs of divesting firms in the context of the Sarbanes-Oxley Act of 2002 (SOX). We hypothesize that firms with higher corporate divestiture intensities are more likely to have material weaknesses in their IT controls, more likely to become incompliant with SOX, and more likely to incur higher auditor fees during SOX audits. We also hypothesize that superior IT capabilities could reduce the probability and magnitude of the regulatory compliance risks and costs during divestitures. We find empirical support for these hypotheses in a sample of 252 publicly traded U.S firms that were audited independently for SOX compliance between 2004 and 2008.

Keywords: IT disintegration, corporate divestitures, IT control effectiveness, Sarbanes-Oxley compliance, auditor fee, IT capability

Introduction

Integrating IT systems and processes within and across firm boundaries is an important task of IT functions of corporations (Barki and Pinsonneault 2005). IT integration enhances connectivity, communication, collaboration, and coordination within and across firm boundaries, and generates synergy and performance benefits. IS research recognizes the importance of IT integration and studies its antecedents and consequences in strategic initiatives of firms such as corporate diversification (Tanriverdi 2005), mergers and acquisitions (Mehta and Hirschheim 2007), strategic partnerships and inter-firm relationships (Kim and Mahoney 2006; Malhotra et al. 2007; Rai et al. 2006; Saraf et al. 2007), and outsourcing and offshoring (Lee et al. 2004; Tanriverdi et al. 2007). A phenomenon that has not received much research attention is that firms not only need IT integration, but, on a selective basis, they also need IT disintegration (Markus 2000). Selling-off a business unit, changing strategic alliance partners, bringing back in-house previously outsourced or offshored IT or business operations, or internally reconfiguring relationships among business units are examples of business decisions that require the IT function to engage in disintegration of some of the previously integrated IT systems and processes. As Lynne Markus (2000) suggests, "*[t]oday, management philosophy emphasizes business disintegration as much as (or more than) it does business integration.*" While IS research has studied IT integration extensively, it has paid very little attention to IT disintegration (Markus 2000; Markus 2001). In this research, we begin addressing this gap by studying some of the risks and costs associated with IT disintegration requirements of corporate divestitures.

IT disintegration during corporate divestitures entails notorious IT challenges. During divestiture, one firm sells-off one of its business units to another firm as an individual operating unit (Decker and Mellewigt 2007). In their daily operations, companies are pursuing IT integration for cross-unit integration, coordination, and synergy creation (Tanriverdi 2006). However, the dominant system integration paradigm tends to tightly couple IT resources through ad hoc middleware or monolithic software packages such as ERP (Rettig 2007). Such integration approaches raise barriers to disintegration of IT resources during divestitures. As Markus argues: "*[w]hat happens when companies are divested or spun off? Huge efforts are often required to disconnect their operations from those of parent companies…Today's systems integration paradigm does not afford this capability*" (Markus 2001). Not surprisingly, Booz Allen Hamilton (2002) lists IT disintegration as one of the top challenges in corporate divestitures. AT Kearney (2004) reinforces this observation by stating, "*In nearly all of our divestiture projects, information technology has been the most complex and difficult area to separate, and the time required for separation has always been underestimated.*" Deloitte Consulting (2009) attributes the IT disintegration challenges to the IT integration wave fueled by ERP implementations: "*[a]s a result of the trend toward tightly-integrated businesses largely driven by ERP implementations over the past 20 years, carving out and divesting business units have become more complex…significantly more planning and resources are required to create a stand-alone business unit.*" Divestiture performance could be significantly weakened if the seller underestimates the costs of IT disintegration. For example, when selling its vitamins division, Roche underestimated the IT disintegration costs by a factor of 20 (Applegate et al. 2007).

IT disintegration challenges during divestitures can disrupt existing IT controls and increase IT risks. For example, divesting firm needs to terminate access to IT systems of all employees leaving with the divested unit. Such bulk access de-provisioning is difficult to complete in a short period. Many orphaned accounts can remain hanging around in the IT systems after the divestiture, and increase the vulnerability of the IT systems to unauthorized access. A recent survey shows that "*10% of terminated individuals sampled were found to have active access on at least 1 key financial system. Half of those were found to also have an active VPN account*" (Sailpoint 2009). Divestitures can also potentially increase other IT risks such as (1) IT competence erosion due to loss of accumulated IT knowledge or capable IT employees, (2) infrastructure risk due to security and access vulnerabilities, (3) IT project risks due to change in ownership and subsequent changes in controller-controlee relationships, (4) business continuity risks due to disruption of operations during the separation of previously integrated systems and processes, and (5) information risks such as the loss of protection of data privacy and intellectual property due to disruption of related controls during the change management processes of divestitures (Parent and Reich 2009).

In this study, we examine how IT disintegration challenges faced in corporate divestitures affect regulatory compliance risks and costs of divesting firms in the context of the Sarbanes-Oxley Act (SOX) in the U.S. SOX provides an appropriate empirical context for this study because section 404 of the Act (SOX-404) requires management of publicly traded U.S. firms to disclose an assessment of the state of the firm's internal controls over financial reporting. It also requires independent auditors of the public firms to attest to the managements' assessments of internal controls. Controls over IT activities and IT-enabled automated process controls are integral parts of this assessment (ITGI 2006). Thus, with the passage of the Act in 2002, IT control effectiveness assumed top priority in the agendas of CEOs, CFOs, and CIOs in large publicly traded firms. An IT executive reported, "*SOX forced a major reprioritization of everything from top to bottom*" (Parry 2004). Another IT executive reported that he had to spend about 35% of his time getting ready for the SOX compliance deadline. It is important for firms to prevent material weaknesses in their IT-based and non-IT internal controls for several reasons. First, capital markets negatively react to disclosures of internal control material weaknesses (ICMW) (Beneish et al. 2008; Hammersley et al. 2008). Second, ICMW adds noise to accounting information and leads to unintentional accounting treatment errors such as inaccurate accruals (Ashbaugh-Skaife et al. 2008). Third, ICMW increases audit fees charged by the external auditors (Raghunandan and Rama 2006). Fourth, ICMW could increase firm's risk of being de-listed from the stock exchange by regulators, and the CEOs and CFOs of publicly traded firms face the risk of being fined up to $5million and being jailed for up to 20 years under certain circumstance. Thus, firms have invested significantly in IT and non-IT internal controls to become compliant with SOX-404 for the first time. But, SOX compliance is not a one-time event. It is an ongoing process since firms are required to maintain their compliance with SOX every year. Corporate restructuring activities such as divestitures, mergers, and acquisitions could potentially disrupt a previously effective internal control system (Ashbaugh-Skaife et al. 2007), and as a result, increase the risk of noncompliance and costs of compliance. The internal control system must be updated to match the restructured business portfolio (Doyle et al. 2007).

Studies focusing on determinants and consequences of ICMW find that firms with ICMW disclosures tend to be smaller, younger, financially weaker, more complex, more active in restructurings, change more rapidly, and have more accounting risks (Ashbaugh-Skaife et al. 2007; Doyle et al. 2007). They tend to have more prestigious and more independent external auditors, more concentrated ownership, auditing committees that are more knowledgeable in accounting and finance, and histories of financial report restatements and auditor resignations (Ashbaugh-Skaife et al. 2007; Zhang et al. 2007). As this literature review indicates, prior research did not study IT related determinants and consequences of ICMW. A few notable exceptions are Li et al (2007), who find that the presence of IT expertise in the top management team and audit committee of a firm reduces the likelihood of IT control weaknesses; Grant et al (2008), who show that IT control weaknesses have pervasive impact on financial reporting; and Canada et al. (2009), who investigate the relationship between IT control weaknesses and audit fees. In this paper, we seek to contribute to this nascent, but important literature stream by explaining how "IT" could both be the source of the ICMW problem and a potential solution to it. Specifically, we argue that IT disintegration challenges entailed in corporate divestitures can create problems by reducing the effectiveness of firms' IT controls and increasing the firms' risks and costs in SOX compliance. We also posit that superior IT capabilities could potentially serve as one solution mechanism by mitigating the negative effects of corporate divestitures on SOX compliance risks and costs of firms.

Constructs and Hypotheses

IT control effectiveness

Internal controls are defined as "*the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected*" (ITGI 2007). Modern firms rely heavily on IT applications to support their business policies, processes, and practices. Some managerial controls that are designed to mitigate potential risks to the achievement of business objectives are automated into the IT applications. We refer to them as IT-enabled or automated process controls. For example, a firm can implement the "three-way match" process as an internal control mechanism to reduce the risk of paying for goods that are billed by suppliers but not received by the firm. If the firm automates its order, shipment, inventory, and payment processes, it can automatically implement the three-way match process in its IT systems. In addition, there are potential risks in the underlying IT resources and IT management processes of a firm. IT resources and management processes should also be controlled to ensure that they perform as intended and deliver the expected functionality with high accountability. Firms implement IT general controls to mitigate IT related risks in their IT environments, computer operations, access to IT applications and data, application development, and program changes (ITGI 2006). Thus, there are two types of IT controls: (a) IT-enabled, automated business controls (IIA 2005); and (b) controls over IT resources and management processes, or, IT general controls (ITGI 2006).

SOX-404 demands the assessment of the effectiveness of internal controls over financial reporting, including automated business controls and IT general controls. The effectiveness of the internal controls in the SOX context is defined as the extent to which the internal control system can reduce the possibility of material misstatement of financial reports of a firm. During a SOX-404 audit, external auditors analyze a firm's internal controls (IT and non-IT), financial reporting processes, and map the underlying IT environment that supports the internal controls and financially significant processes and accounts. They also test whether the controls are working effectively as intended. Based on their auditing standards, independent auditors conclude SOX-404 audits with a decision about the effectiveness or ineffectiveness of the firm's internal controls.

The problem: Why do IT disintegration requirements of corporate divestitures negatively impact IT control effectiveness, SOX compliance, and auditor fees of divesting firms?

In integrating IT systems of units, firms seek to establish linkages among previously distinct and autonomous IT resources of the units and make them function as a unified whole (Barki and Pinsonneault 2005; Markus 2000). IT disintegration reverses this process. IT disintegration during a divestiture refers to the process of disentangling previously unified IT resources of the divested unit from the divesting firm for independent operation. Unified, interdependent IT resources of the two businesses are split up into distinctive parts to separately serve the divested and divesting businesses. IT resources in the divesting business are adapted and scaled down to match the shrinking business requirements (Gartner 2005).

The risks entailed in IT disintegration during a divestiture depends on the ex ante IT integration status of the divesting firm. If IT and business resources of the divested unit were autonomous relative to those of the other business units of the seller, the divestiture would entail little or no resource reconfiguration and separation. This is rare, however, because most sellers have some degree of cross-business integration and share common IT and business resources across their business units. During normal operation, cross-business resource integration is desirable for a firm because it creates cross-business synergies in the form of reduced costs and increased revenues and improves the overall corporate performance of the firm (Tanriverdi 2005). However, the widely adopted IT integration techniques may create barriers for disintegration. IT could be integrated through (1) data warehouse which connects IT applications by periodically sharing and exchanging data, (2) ad hoc middleware which connects IT applications by translating data flows from one to the other, or (3) a single monolithic software package like ERP which provides most of needed functionality (Markus 2000). The first two approaches create complicated interdependence between IT resources and thus increase the complexity of the overall IT architecture. The third approach assumes that monolithic software like ERP can solve the problems, but it turns out to be just another layer of complexity because it still needs to be integrated with peripheral systems or newly acquired systems and it is rigid to change (Rettig 2007). Customization of pre-packaged software also creates extra complexity by increasing maintenance and upgrade challenges.

The complexity of integrated IT application architecture introduces significant risks for IT disintegration tasks. Banker et al.(1998) found that higher software complexity leads to more project hours of software modification. More complex and volatile software codes need more structures in the software codes to decrease such modification efforts by localizing changes (Banker and Slaughter 2000). However, it then incurs additional efforts to comprehend the structure when the software is modified because maintainers need to trace long chains of interdependence and comprehend complicated interfaces (Banker and Slaughter 2000). Changes in one single application will possibly influence every other linked application which then complicates the overall change management task (Mookerjee 2005). Every integration effort may exponentially increase the challenge of future disintegration, as Banker et al. (1998) describe in the context of software development: "*the key idea is that software development practices have long-term consequences that are difficult and costly to reverse.*" When the divesting firm has a complex system of many IT components that are interacting with each other due to interdependency relationships, a seemingly minor glitch triggered by an IT disintegration activity in one part of the system could potentially propagate through the entire system, amplify along the way, and lead to a system-level catastrophe, as suggested by the "normal accident theory" (Perrow 1999). Different control procedures are recommended for mitigating risks in different phases of an IT project (Kirsch 2004). But in each phase IT risk resolutions needed to mitigate IT project risks may not be identified correctly or executed effectively due to ambiguous heuristics between risk factors and risk resolutions (Lyytinen et al. 1998). Thus, IT disintegration activities during a divestiture could increase the probability of IT control failures. For example, in its 10-K filing in 2007, NiSource Inc. disclosed that it experienced IT control material weaknesses due to its large scale IT system implementations and business process changes: "*many new* *information technology systems and process changes had an accelerated time-line for completion, which created the risk of operational delays, potential errors and control failures which could impact NiSource and its financial condition.*"

IT strategies, policies, management practices and IT human resources of a firm have pervasive influence on the effectiveness of the firm's IT controls (ITGI 2006). During a divestiture, disintegration of managerial IT resources such as the separation of IT executives, IT human resources, IT strategies, policies and processes of the divesting firm and the divested unit could disrupt the effectiveness of the IT controls. In software engineering literature, Boehm (1991) lists personnel shortfalls and straining computer science capabilities as two major risk factors in software projects. In the accounting literature, Ashbaugh-Skaife and her colleagues (2007) argue that firms participating in downsizing usually face internal control risks such as the lack of segregation of duties and inadequate staffing and supervision. Prior to the divestiture, managerial IT resources such as the CIO, IT human resources, IT strategies, policies and processes are shared and integrated across multiple units of the firm. Some of key IT employees of the firm are likely to leave along with the divested unit, and the remaining ones may experience a higher turnover rate than usual because of the jobs uncertainty created by the divestiture (Kay and Shelton 2000). IT management policies need to be updated to match the new business and IT environment of the divesting firm. The adaptation of an established internal control environment in a short transition period is a risky and costly initiative (Doyle et al. 2007) which increases the probability of ineffective IT controls. Thus, as the divestiture intensity of a firm increases, i.e., the firm disentangles and sells a higher percentage of its overall business portfolio, IT controls of the firm will become more likely to decline in effectiveness and experience material weaknesses. In SOX-404 audits, the detection of material weaknesses in IT controls of a firm is by definition considered to be a failure to comply with the regulation. Thus, we expect increasing divestiture intensity of a firm to reduce the firm's likelihood of compliance with SOX-404 by reducing IT control effectiveness of the firm:

H1a: Increasing divestiture intensity of a firm reduces the firm's IT control effectiveness.

H1b: Increasing divestiture intensity of a firm reduces the firm's likelihood of compliance with SOX-404.

Internal control disruptions and weaknesses caused by corporate divestitures are also likely to increase compliance costs incurred by the divesting firm during a SOX-404 audit. One major source of SOX compliance costs is due to the involvement of independent auditors. Auditor fees include audit fees paid to the independent auditor of the firm for the auditing services and the non-audit service fees paid to accounting firms for advisory services. The detection of internal control exceptions and deficiencies creates significant additional work for external auditor of the firm and increases the audit fees. During financial audits, if an internal control exception is detected, auditors will have to increase their substantive testing of financial transactions rather than relying on a simple walkthrough test or tests of smaller samples. The presence of an IT control exception implies even more work for auditors because if the underlying IT systems are not reliable, business processes that run on them or the financial information generated by them are not reliable either. Auditors have to conduct more substantive testing, change their audit program, communicate more with managers of the firm, and they have to assess and document the severity of the IT control exception (Raghunandan and Rama 2006). As a result, they will charge higher auditor fees. Prior research finds that firms with material weakness disclosures pay higher fees to external auditors compared to firms without such disclosures (Ettredge et al. 2007; Raghunandan and Rama 2006). Firms with IT control material weaknesses also pay higher audit fees (Canada et al. 2009). In this study, we seek to extend these findings by explaining that corporate divestitures increase auditor fees by reducing the effectiveness of IT controls. A firm can manage to prevent material weaknesses caused in its IT controls by a divestiture, and as a result, it can remain compliant with SOX-404 despite the divestiture. However, it is still likely to incur higher auditor fees because divestitures disrupt the IT controls, and lead to "deficiencies" or "significant deficiencies," less severe forms of exceptions in them. Thus:

H1c: Increasing divestiture intensity of a firm increases auditor fees of the firm.

One potential solution: How do superior IT capabilities mitigate the negative effects of divestitures on IT control effectiveness, SOX compliance, and auditor fees of divesting firms?

We propose superior IT capabilities as one potential solution to the IT disintegration problems caused by corporate divestitures. Following prior studies, we define IT capability as the firm's "*ability to mobilize and deploy IT-based resources in combination or copresent with other resources and capabilities*" (Bharadwaj 2000). IT capabilities are dynamic capabilities that enable firms to develop, add, integrate, and release key IT and business resources over time (Wade and Hulland 2004). Thus, they are critical to the successful restructuring of business portfolios.

IT disintegration in corporate divestitures requires major IT resource reconfiguration and change management processes. Sellers must be meticulous about planning how the IT disintegration will unfold, define boundaries of the divested business, determine which specific IT systems and processes will be separated from the company and transferred to the divested unit. Cross-company IT systems and processes need to be carefully unraveled to ensure effective separation (Mankins et al. 2008). Old IT systems and processes will need to be split off, retained, terminated, or replaced with new ones to ensure the independent operation of the divesting and divested organizations (Gartner 2005). To reconfigure the business processes, all firms needs a basic level of IT capability to implement the changes. More pervasive changes will require higher levels of IT capabilities (Broadbent et al. 1999). Firms with superior IT capabilities have well-defined, documented, standardized, and repeatable processes for managing changes in their IT infrastructures and applications. Hence, they are likely to better address the IT disintegration challenges of corporate divestitures and better mitigate the risks and costs associated with them compared to firms that lack strong IT capabilities. For example, a firm with superior IT capability has a well-defined IT planning and organization process, which can be leveraged in the pre-divestiture due diligence phase of corporate divestitures. With a well-defined IT planning and organization process, the firm can plan the IT disintegration activities of the divestiture, assess potential risks to the successful implementation of the IT disintegration activities, and develop control objectives and control activities for mitigating the risks.

A superior IT capability can also potentially mitigate the negative effects of divestitures on the firm’s ability to comply with SOX-404. IT systems and processes support and complement the business systems and processes. Thus, when a superior IT capability addresses challenges and threats posed by IT disintegration activities of a divestiture, the improvements in IT control effectiveness will also positively reinforce the effectiveness of overall internal controls. For example, if the divestiture disrupts the existing IT controls and creates vulnerabilities in IT security controls, IT access controls, IT change management controls, and segregation of duties in the IT infrastructure, the digitized business processes that run on the IT infrastructure will also be vulnerable to malicious activity such as hacking, fraud, and manipulation. External hackers or disgruntled employees inside the firm can exploit the IT control deficiencies to breach business controls as well and gain unauthorized access to financially significant business processes. However, firms with superior IT capabilities are more likely to identify and fix the IT control deficiencies. The improvements in IT control effectiveness will positively reinforce the effectiveness of the business controls as well. Thus, we expect firms with superior IT capabilities to be more likely to reduce the negative effects of divestitures on their IT control effectiveness and ability to comply with SOX-404.

H2a: A superior IT capability reduces negative effects of divestitures on firm’s IT control effectiveness.

H2b: A superior IT capability reduces negative effects of divestitures on firm’s SOX-404 compliance.

In auditing financially significant business processes, external auditors pay close attention to the underlying IT infrastructures and applications. If there are security holes in the IT infrastructure or applications supporting the business processes, the auditors cannot rely on the data generated by the business processes. Then, instead of sampling and testing a subset of the transactions, they may have to examine the entire set of transactions carefully because the control deficiencies in the underlying IT systems and applications significantly increase the risk of fraudulent transactions. Since external auditors increase their work significantly, the audit fees they charge to the firm will also increase. As discussed above, IT disintegration requirements of corporate divestitures will disrupt the effectiveness of IT controls and lead to the escalation of the audit fees and non-audit advisory service fees. While the escalation of these costs may be inevitable in the context of IT disintegration challenges of corporate divestitures, a firm can mitigate the escalation of the costs by developing superior IT capabilities for identifying and fixing the identified IT control deficiencies. Firms with weaker IT capabilities have to incur higher audit fees because they have to hire the services of external firms and pay advisory fees to remedy the IT control deficiencies caused by divestitures. Thus:

H2c: A superior IT capability reduces the escalation effects of increasing divestiture intensity on auditor fees of the firm.

Methods

Sample and data

Our sampling frame for this study are all firms tracked by Audit Analytics, which maintains a database of independent auditors' annual assessment opinions on the effectiveness of internal controls of publicly traded firms that are subject to the SOX regulation. Audit Analytics also track auditor fees. Our timeframe covers November 2004, the earliest SOX-404 compliance deadline, and December 2008, the latest observation available as of this writing. If an independent auditor issues an adverse opinion for internal controls of a firm, the type of internal control weakness is reported in the Audit Analytics database. This enables us to capture if a firm had material weaknesses in its internal controls, and hence, was incompliant with SOX-404 in a given year. The database also reports material weaknesses in IT controls of firms under code #22. Specifically, the database describes code #22 as a material weakness arising from an "Information technology, software, security, and access issue." Thus, we are able to use code #22 to identify if IT controls of a firm were effective (=1) or not (=0) in a given year. In our study timeframe, a superset of 205 unique firms were incompliant with SOX-404 and they disclosed a total of 276 IT control material weaknesses.

Matching process

Our purpose is to test whether divestiture intensities and IT capabilities of firms affect their IT control effectiveness, SOX-404 compliance, and auditor fees. After identifying the main sample of firms that were incompliant with SOX-404 and had IT control material weaknesses, we also constructed a matched sample of firms, which exhibited similar organizational characteristics, but were compliant with SOX-404 and had effective IT controls. Following Barber and Lyon (1996), for each firm in our main sample, which received an ineffective SOX-IT evaluation (=0) at time (t), we go back two years in time to (t-2) and search for a control firm, which was in the same industry and had similar financial performance with that of the sample firm as of (t-2), but ended up with an effective SOX-IT evaluation (=1) at time (t). This approach enables us: (a) to have even dispersion in our dependent variables (e.g., about 50% of the combined sample is SOX-IT compliant, whereas the other 50% is incompliant); (b) build a two-year lag structure between our main independent variable (divestiture intensity) and the dependent variable; and (c) test whether the variance in divestiture intensities of the firms within two years of the compliance date (t-2, t) explains variance in the firms' abilities to comply with SOX-IT requirements at time (t).

We followed the steps suggested by Barber and Lyon (1996) to construct the matched control sample. The construction process is summarized in Table 1 below.

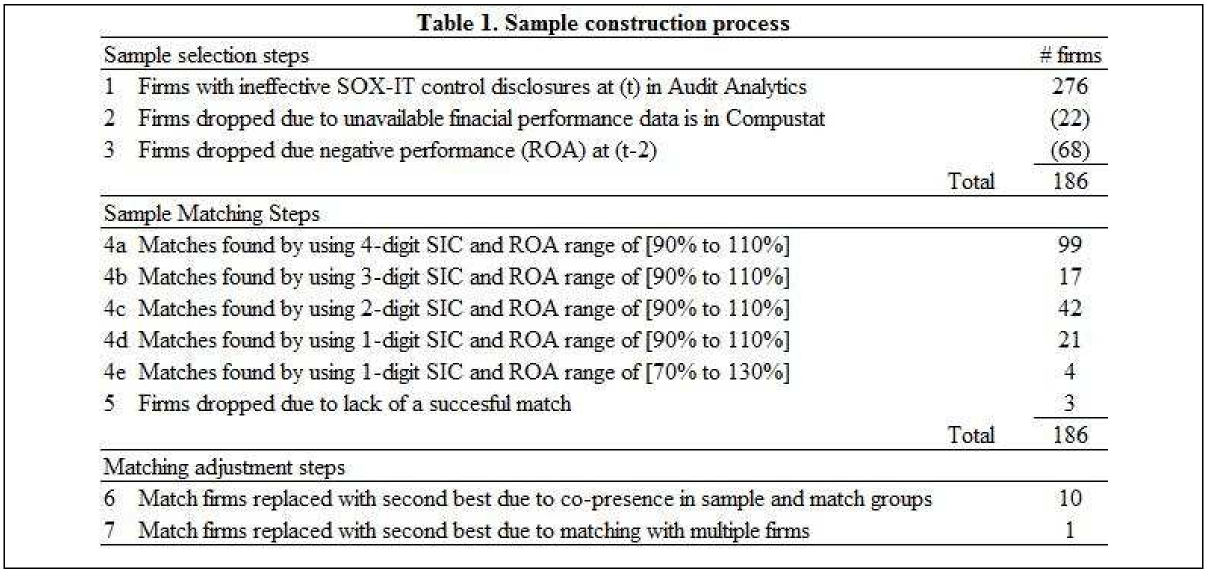

Table 1. Sample construction process

Sample selection steps		# firms
1	Firms with ineffective SOX-IT control disclosures at (t) in Audit Analytics	276
2	Firms dropped due to unavailable finacial performance data is in Compustat	(22)
3	Firms dropped due negative performance (ROA) at (t-2)	(68)
	Total	186
Sample Matching Steps		
4a	Matches found by using 4-digit SIC and ROA range of [90% to 110%]	99
4b	Matches found by using 3-digit SIC and ROA range of [90% to 110%]	17
4c	Matches found by using 2-digit SIC and ROA range of [90% to 110%]	42
4d	Matches found by using 1-digit SIC and ROA range of [90% to 110%]	21
4e	Matches found by using 1-digit SIC and ROA range of [70% to 130%]	4
5	Firms dropped due to lack of a succesful match	3
	Total	186
Matching adjustment steps		
6	Match firms replaced with second best due to co-presence in sample and match groups	10
7	Match firms replaced with second best due to matching with multiple firms	1

First, we started with the main sample of firms which had ineffective SOX-IT control disclosures in the Audit Analytics database (276 firm-year observations). Second, we focused on a subset of those firms for which data on one of our matching criteria, i.e., financial performance, was available in Compustat (254 firm-year observations). Third, we selected firms whose financial performance was positive (186 firm-year observations). Imposing this criterion ensured that firms in our sample divested one of their business units not because of poor previous performance of the unit, but because of a strategic intention. Thus, we use a conservative sample of profitable firms engaging in corporate portfolio transformations for strategic reasons. Following (Barber and Lyon 1996), we measure financial performance by return on assets (ROA) and compute it as operating income (Compustat Item OIBDP) divided by the average of beginning- and end-of-period total assets (Compustat Item AT). Fourth, we focus on a subset of the candidate control firms in the Audit Analytics database that were operating in the same SIC industry as the sample firm in year (t-2) and achieved SOX-IT compliance in year (t). The industry match controls for cross-sectional variations in operating performance that arise from industry. Following Barber and Lyon (1996), we try to identify a firm whose performance was within 90% to 110% range and closest to that of the sample firm's ROA at year t-2 in the firm's 4-digit SIC industry. For the remaining unmatched firms, we check if we can find a match in the same 3-digit SIC, or 2-digit SIC, or 1-digit SIC. For the firms that still remain unmatched, we follow Baber and Lyon's (1996) suggestion to expand the performance range to 70% to 130% of the sample firm's ROA. We have to drop three firms because we cannot find a match for them despite the steps above. We checked if any control firms happened to be in our main sample. We identified 10 such firms and replaced them with the second closest match. Finally, we replaced one more matched firm, which was selected as a match to multiple firms in the main sample. We performed independent t-tests to compare differences between the sample and the matched control firm characteristics. The two groups are not significantly different along our matching criteria, the ROA (t=.092, p>0.1). This indicates that the matching process worked as intended. After collecting data on all study variables and missing some more observations due to missing data, we were able to retain for hypothesis testing a sample size ranging from 228 to 293 dependent on different models.

Dependent Variables

IT control effectiveness. As noted above, we measure IT control effectiveness of a firm by code #22 in the Audit Analytics database. While this dummy variable may appear simplistic, external auditor of a firm conducts independent assessments of hundreds of IT controls of the firm before concluding if the overall IT controls of the firm are effective (=1) or not (=0). This assessment is disclosed to regulators and the investing public. Thus, it is the most comprehensive and objective measure of a firm's IT control effectiveness that is publicly available. In some cases, a firm's SOX-404 report is restated multiple times in a year (observed in 4.6% of the sample). In such cases, we use the latest audited results.

SOX-404 Compliance. We perform the matching work based on IT control weakness, and by definition all the observations in the IT control weakness group are incompliant. In the control group, 15 firms are also incompliant with SOX-404 due to non-IT control weaknesses. To test if IT disintegration challenges of divestitures affect SOX-404 compliance as hypothesized, we include a firm's SOX-404 compliance (1=compliant) as our second dependent variable. We measure it with independent auditor's assessment of the firm's internal control over financial reporting as publicly disclosed in SEC annual filings and recorded in the Audit Analytics database.

Auditor fees. Our third dependent variable of interest for assessing the problems created by IT disintegration challenges of divestitures is the amount of auditor fees (audit fees plus non-audit advisory fees) paid by the divesting firm. We obtain auditor fee data from the Audit Analytics database and compute the logarithm of total auditor fees paid to auditors within two years of the SOX-IT control disclosure date (t-2,t).

Explanatory Variables

Divestiture intensity. We measure divestiture intensity as the percentage of the firm's total business portfolio that is divested within two years of the SOX-IT control disclosure date. Transaction values of all selected divestitures of the firm in the past two years (t-2, t) are summed and then divided by the market capitalization of the firm at the end of year (t-2). Since the sizes of divested units vary greatly relative of the size of the seller, to ensure that we focus on significant divestitures, we select only those whose individual transaction volumes are larger than 10% of the firms' market capitalization, or when a series of divestitures within the two year time window jointly account for more than 10% of the firms' market capitalization. We collect data on divestiture activity of firms from the SDC Platinum database and year-end market capitalization data from CompuStat database.

IT capability. We use objective, publicly available measures of firms' IT capabilities as assessed by the Information Week (IW) magazine. In creating its annual list of IW500 firms, IW asks a panel of IW experts and industry peers of candidate firms whether IT capabilities of the candidate firms are above-average in their respective industries in terms of their patterns of technological, procedural, and organizational innovation. If a firm is selected into the IW500 list, it is considered to have superior IT capabilities relative to its industry peers. This measure of IT capability has been used in prior IS studies (e.g., Bharadwaj 2000; Radhakrishnan et al. 2008; Sabherwal and Sabherwal 2005; Santhanam and Hartono 2003). We consider a firm in our sample as having a superior IT capability if it appears in the IW500 list in the five-year time window prior to the firm's SOX disclosure date.

Control Variables

Industry-adjusted sales growth. Rapidly growing firms may fail to timely update their internal controls and encounter staffing issues. Newly established procedures in rapidly growing firms are also more likely to have deficiencies (Ashbaugh-Skaife et al. 2007; Doyle et al. 2007). Thus, we control for sales growth of firms and compute it by sales (CompuStat Item SALE) growth of firm at year (t-2) minus average sales growth of the firm's industry in the same period.

Firm size. Large firms are likely to have more resources to invest on their internal controls and hire adequate number of employees to ensure proper segregation of duties (Ashbaugh-Skaife et al. 2007; Doyle et al. 2007). Thus, we control for size of firms and operationalize it as the logarithm of firm's market capitalization. Our results are robust to alternative size measures such as logarithm of number of employees or logarithm of total assets.

Foreign operation. Firms that have foreign operations face different institutional and legal environments and have more complex transactions. Following prior studies (Ashbaugh-Skaife et al. 2007; Doyle et al. 2007), we control for foreign operations of firms by including a dummy variable taking on a value of [1] when a firm has a foreign currency adjustment in its financial statement, [0] otherwise.

Inventory level. Prior studies on internal control effectiveness also control for firm's relative level of inventory to capture accounting measurement application risks (Ashbaugh-Skaife et al. 2007; Ogneva et al. 2007). Firms with more inventories face more risks related to inventory measurement, recording, reporting and valuation (Ashbaugh-Skaife et al. 2007). Thus, we control for inventory level by computing the ratio of [inventory (Compustat Item INVT)] / [Total assets (Compustat Item AT)].

IT intensity. Firms operate in different industrial environments having different levels of IT intensity. In IT-intensive environments, firms may have more exposures to IT risks and their divestitures may require more IT disintegration activity. Thus, we control for IT intensity of firms. First we compute IT intensities of the industry segments in which a firm participates. IT intensity of an industry segment is measured as the ratio of the software and hardware stock value over the total equipment stock value in the segment (Brynjolfsson et al. 1994). Data on IT and other equipment stock is obtained from the Bureau of Economic Analysis (BEA). Then, we compute a firm level IT intensity measure by using the firm's percentage of sales generated from a segment as weight and computing a sales weighted average of IT intensities of all industry segments in which the firm operates. Data on sales distributions of firms across segments is obtained from Compustat's segment database.

Diversification level. Diversified firms may face more challenges in maintaining effective IT controls due to their heterogeneous IT environments. In addition, they tend to restructure their business portfolios more frequently. To account for these effects, we control for the diversification level of firms in our sample. We adopt the entropy measure of total diversification suggested by Palepu (1985), and compute it as $\sum_{i=1}^{N} P_i \ln(1/P_i)$, where P_i is the share of the i th segment of the firm in the total sales of the firm. The data for this measure is obtained from Compustat's segment database.

M&A intensity. Firms may divest businesses as a consequence of previous mergers or acquisitions (Bergh 1997; Shimizu and Hitt 2005). Post acquisition integration could also introduce internal control weaknesses (Ashbaugh-Skaife et al. 2007; Doyle et al. 2007). To account for the effects of M&A, we control for M&A intensity and compute it as the summed M&A transaction volumes of a firm in the past three years divided by the firm's market capitalization in the SOX-IT control disclosure year. The three-year time window is one year longer than the two-year window used for divestitures. This allows us to capture if the divestitures of interest in our sample were due to earlier M&A activity of the firm. Data on M&A transactions of firms is obtained from the SDC Platinum database.

Unless stated otherwise, we measure all control variables two years before the dependent variables to account for reverse causality and possible endogeneity biases. Table 2 presents descriptive statistics and correlations among the study variables.

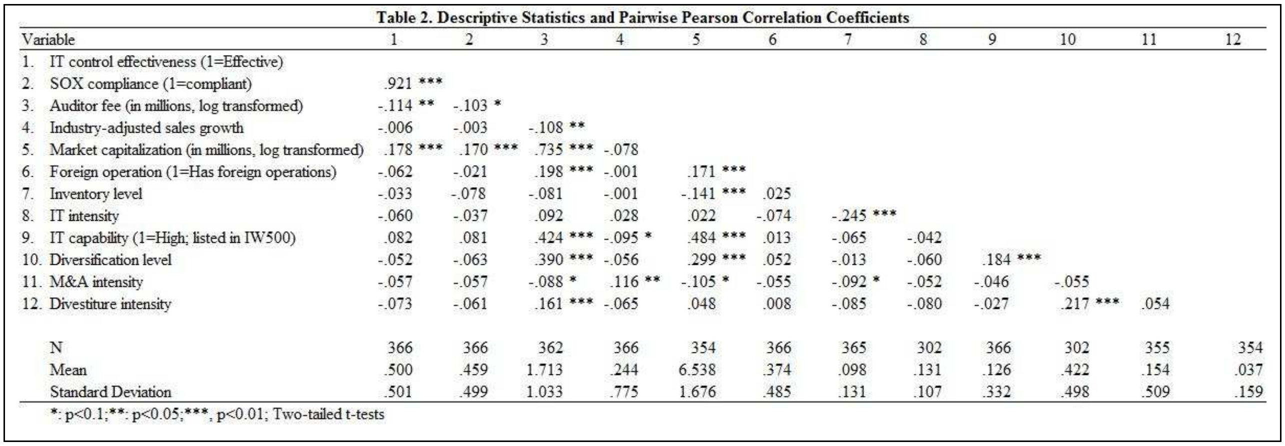

Table 2. Descriptive Statistics and Pairwise Pearson Correlation Coefficients

Variable	1	2	3	4	5	6	7	8	9	10	11	12
1. IT control effectiveness (1=Effective)												
2. SOX compliance (1=compliant)	.921 ***											
3. Auditor fee (in millions, log transformed)	-.114 **	-.103 *										
4. Industry-adjusted sales growth	-.006	-.003	-.108 **									
5. Market capitalization (in millions, log transformed)	.178 ***	.170 ***	.735 ***	-.078								
6. Foreign operation (1=Has foreign operations)	-.062	-.021	.198 ***	-.001	.171 ***							
7. Inventory level	-.033	-.078	-.081	-.001	-.141 ***	.025						
8. IT intensity	-.060	-.037	.092	.028	.022	-.074	-.245 ***					
9. IT capability (1=High; listed in IW500)	.082	.081	.424 ***	-.095 *	.484 ***	.013	-.065	-.042				
10. Diversification level	-.052	-.063	.390 ***	-.056	.299 ***	.052	-.013	-.060	.184 ***			
11. M&A intensity	-.057	-.057	-.088 *	.116 **	-.105 *	-.055	-.092 *	-.052	-.046	-.055		
12. Divestiture intensity	-.073	-.061	.161 ***	-.065	.048	.008	-.085	-.080	-.027	.217 ***	.054	
N	366	366	362	366	354	366	365	302	366	302	355	354
Mean	.500	.459	1.713	.244	6.538	.374	.098	.131	.126	.422	.154	.037
Standard Deviation	.501	.499	1.033	.775	1.676	.485	.131	.107	.332	.498	.509	.159

*: p<0.1;**: p<0.05;***, p<0.01; Two-tailed t-tests

Model Specification

Because we adopted a matched control sample technique and two of our dependent variables are binary variables, a conditional Logit model is appropriate to capture the matching structure within the sample. Under conditional Logit model and using a dataset consisting of one-to-one matched pairs, the conditional likelihood is specified as (Breslow 1982):

$$\prod_{i=1}^{I} \frac{1}{(1+\exp((\mathbf{x_{i1}}-\mathbf{x_{i0}})'\boldsymbol{\beta}))}$$

where $\mathbf{x}_{i1}$ and $\mathbf{x}_{i0}$ are row vectors consisting of all the explanatory variables for the sample and the control firms in ith matched pair, I is the total number of pairs, and $\boldsymbol{\beta}$ is a column vector of corresponding coefficients to be estimated. Compared to the regular Logit, a conditional Logit model calculates the likelihood of the binary outcomes conditional on each matched pair. This estimation method is widely used by biostatisticians and epidemiologists to perform case-control studies (Breslow 1982; Hosmer and Lemeshow 2004), and also adopted in accounting research (Cram et al. 2007; Zhang et al. 2007). We use robust standard errors clustering on firms and their pairs to allow interdependence of observations between them (Stata 2007).

For our third dependent variable, auditor fees, we use OLS regression with the same robust standard error structure. Multicollinearity tests on these linear models show that the VIFs in all the OLS models are below 3, which is far below the suggested threshold 10. The results on each of the three dependent variables are presented respectively in panels A, B, and C of Table 2. In each panel, the first model enters the control variables. The second model enters the main effect of divestiture intensity. Finally, the third model enters the moderation effect of IT capability.

Results

Table 3 below summarizes the statistical results. Divestiture intensity of a firm has negative and significant impacts on IT control effectiveness (Panel A, second model) and SOX-404 compliance of the firm (Panel B, second model). It also increases auditor fees (Panel C, second model). Thus, H1a, H1b, and H1c are supported.

IT capability moderates the relationships between (1) divestiture intensity and IT control effectiveness (Panel A, third model); (2) divestiture intensity and SOX-404 compliance of the firm (Panel B, third model); and (3) divestiture intensity and auditor fees of the firm (Panel C, third model). Thus, H2a, H2b, and H2c are also supported.

The overall model statistics are significant as indicated by the Likelihood Ratio test statistics for conditional Logit models and model F statistics for OLS regressions.

Table 3. Impacts of divestitures and IT capability on effectiveness of internal controls and auditor fees

Dependent Variables on Panels A, B, and C	Panel A. IT control effectiveness (1=Effective)			Panel B. SOX Compliance (1=Compliant)			Panel C. Auditor fees		
Explanatory Variables	**Controls**	**Main Effect of Divestitures**	**Moderation Effect of IT Capability**	**Controls**	**Main Effect of Divestitures**	**Moderation Effect of IT Capability**	**Controls**	**Main Effect of Divestitures**	**Moderation Effect of IT Capability**
Constant							-1.058 ***	-1.089 ***	-1.095 ***
							(.355)	(.356)	(.356)
Industry-adjusted sales growth	-.171	-.239	-.260	-.198	-.277	-.296	-.053	-.046	-.046
	(.140)	(.157)	(.170)	(.148)	(.184)	(.203)	(.052)	(.049)	(.049)
Firm size (log of market capitalization)	.460 ***	.471 ***	.496 ***	.450 ***	.457 ***	.477 ***	.360 ***	.362 ***	.361 ***
	(.137)	(.138)	(.143)	(.136)	(.136)	(.141)	(.050)	(.050)	(.049)
Foreign operation (1=Has foreign operations)	-1.056 ***	-1.057 ***	-1.154 ***	-.913 **	-.912 **	-1.014 **	.279 ***	.274 ***	.270 ***
	(.375)	(.371)	(.385)	(.400)	(.395)	(.410)	(.099)	(.099)	(.099)
Inventory level	.654	.436	.489	.786	.509	.549	.153	.219	.230
	(1.890)	(1.807)	(1.868)	(2.045)	(1.928)	(2.000)	(.260)	(.269)	(.272)
IT intensity	-5.674 **	-5.637 *	-6.408 **	-3.494	-3.225	-3.857	1.080	1.151	1.192
	(2.899)	(2.925)	(3.153)	(2.391)	(2.321)	(2.572)	(.915)	(.914)	(.922)
IT capability (1=High; listed in IW500)	.218	.143	-.104	.251	.181	-.041	.168	.183	.210
	(.534)	(.550)	(.510)	(.530)	(.538)	(.508)	(.212)	(.211)	(.218)
Diversification level	-.847 **	-.663	-.666	-.983 **	-.793 *	-.792 *	.382 ***	.342 ***	.349 ***
	(.380)	(.405)	(.406)	(.401)	(.425)	(.426)	(.091)	(.097)	(.097)
M&A intensity	-.249	-.259	-.269	-.210	-.219	-.228	-.031	-.043	-.044
	(.220)	(.223)	(.230)	(.214)	(.216)	(.221)	(.047)	(.044)	(.044)
Divestiture intensity		-1.842 *	-2.246 **		-1.884 *	-2.277 **		.580 ***	.653 ***
		(.980)	(1.050)		(1.005)	(1.110)		(.221)	(.226)
Divestiture intensity * IT capability			121.433 ***			121.940 ***			-.881 *
			(7.405)			(7.699)			(.478)
Number of observations	252	252	252	228	228	228	293	293	293
Log-likelihood value	-72.526	-71.489	-69.105	-66.578	-65.556	-63.363			
LR χ^2	22.26 ***	26.48 ***	376.30 ***	20.98 ***	25.30 ***	364.02 ***			
Pseudo R^2	16.96%	18.15%	20.88%	15.74%	17.04%	19.81%			
F-statistics (for Panel C)							38.53 ***	37.72 ***	231.81 ***
R^2 (for Panel C)							56.37%	57.13%	57.27%
ΔR^2 (for Panel C)								0.76% **	0.14%

Notes:
*: p<0.1;**: p<0.05;***, p<0.01; Two-tailed t-tests
Robust standard errors are in parentheses

Discussions and Conclusions

In this research, we identify an important phenomenon that is understudied by IS research: IT disintegration challenges entailed in corporate divestitures. We argue that these challenges create significant risks and costs for the divesting firm. In our empirical study, we choose to examine a subset of those risks and costs in the context of another understudied phenomenon, namely, SOX-404 compliance. Our findings provide support for the proposed theory. IT disintegration challenges entailed in corporate divestitures of a firm reduce the effectiveness of both IT and non-IT internal controls of the firm. They also significantly increase the firm's compliance costs, as captured by external audit fees and non-audit advisory service fees incurred by the firm during its SOX-404 compliance efforts.

In addition to identifying divestitures as a major problem increasing regulatory compliance risks and costs of firms, we identify a potential solution mechanism. Our results on the moderating effect of IT capability indicate that a superior IT capability significantly mitigates the negative effects of divestitures on internal control effectiveness, SOX-404 compliance, and auditor fees. Interestingly, the main effects of IT capability on our dependent variables are not significant. This is an interesting finding for IS research since we tend to assume that IT capabilities are universally valuable. In our study, a superior IT capability does not prevent the regulatory compliance risks or costs associated with IT control disruptions caused by corporate divestitures. But, it does reduce their negative effects.

We contribute to IT security research by linking a strategic move such as corporate divestitures to IT control effectiveness of a firm such as security and access controls, change management controls, controls over computer operations, application development, and so forth. The implication of our findings for IT security research and practice is that no matter how strong a firm's existing security controls and security management capabilities may be, major organizational changes such as corporate divestitures, which entail significant IT disintegration, will disrupt them and increase the firm's compliance risks and costs. However, firms that maintain superior security management capabilities are likely to address and remedy those disruptions more effectively and reduce the negative effects.

Our findings are also important for accounting studies on internal control effectiveness and regulatory compliance. While the accounting research is very much interested in documenting antecedents and consequences of internal control effectiveness, it has not yet identified solution mechanisms for the antecedents that negatively impact internal control effectiveness of firms. Our theory and findings suggest that superior IT capabilities could potentially serve as a viable solution mechanism.

Prior studies recognize that corporate restructuring activities negatively affect internal control effectiveness of firms. However, they focus almost exclusively on mergers and acquisitions and overlook the potential impacts of corporate divestitures. In this study, we sought to introduce corporate divestitures as an additional factor impacting the effectiveness of internal controls, and in particular, the effectiveness of IT controls of firms. In doing so, we followed prior studies and controlled for the effects of M&A intensity of firms as well. Interestingly, our findings on this control variable indicate that M&A intensity does not have any significant effects on internal control effectiveness (IT or non-IT) or auditor fees. Since M&A transactions emphasize IT integration, our findings suggest that the IT disintegration challenges faced in corporate divestitures could be much more consequential for internal control effectiveness and regulatory compliance risks and costs of firms than the IT integration challenges faced in mergers and acquisitions.

Some of our measures are subject to the limitations of archival data. For example, we use the presence or absence of a firm on the IW500 list as an indicator of the firm's superior IT capability or lack thereof. Although this is a widely used measure of IT capability in IS research, it does not provide us detailed insights about the types of IT capabilities divesting firms may be using to address the disruptions caused in their IT controls by a divestiture. Similarly, we use auditor's assessment of the effectiveness or ineffectiveness of IT controls. While auditors go over hundreds of IT controls to make that assessment, they only report material weaknesses, the most severe form of control exception. They do not report less severe forms of control exceptions such as deficiencies or significant deficiencies. Future studies using survey methodology or qualitative methodologies can generate deeper insights about the constructs and nomological relationships examined in this study.

Notwithstanding the data limitations, our theory and preliminary findings in the context of regulatory compliance suggest that IT disintegration is an important topic that is worthy of further research attention. We hope that our study will spark interest in further research on antecedents and consequences of IT disintegration in corporate divestitures, strategic alliances, inter-firm relationships, outsourcing and offshoring arrangements, and internal business portfolio restructuring efforts of firms.

References

Applegate, L.M., Watson, E., and Vatz, M.E. 2007. *Royal DSM N.V.: Information Technology Enabling Business Transformation*. Harvard Business School Case #: 9-807-167.

Ashbaugh-Skaife, H., Collins, D.W., and Kinney Jr, W.R. 2007. "The Discovery and Reporting of Internal Control Deficiencies Prior to SOX-Mandated Audits," *Journal of Accounting and Economics* (44:1-2), pp 166-192.

Ashbaugh-Skaife, H., Daniel, W.C., William R. Kineney, J., and Lafond, R. 2008. "The Effect of SOX Internal Control Deficiencies and Their Remediation on Accrual Quality," *The Accounting Review* (83:1), pp 217-250.

ATKearney. 2004. "Putting out the for-Sale Sign," *Executive Agenda* (7:22), pp 37-43.

Banker, R.D., Davis, G.B., and Slaughter, S.A. 1998. "Software Development Practices, Software Complexity, and Software Maintenance Performance: A," *Management Science* (44:4), pp 433-450.

Banker, R.D., and Slaughter, S.A. 2000. "The Moderating Effects of Structure on Volatility and Complexity in Software Enhancement," *Information Systems Research* (11:3), p 219.

Barber, B.M., and Lyon, J.D. 1996. "Detecting Abnormal Operating Performance: The Empirical Power and Specification of Test Statistics," *Journal of Financial Economics* (41:3), pp 359-399.

Barki, H., and Pinsonneault, A. 2005. "A Model of Organizational Integration, Implementation Effort, and Performance," *Organization Science* (16:2), Mar-Apr, pp 165-179.

Beneish, M.D., Billings, M.B., and Hodder, L.D. 2008. "Internal Control Weeknesses and Information Uncertainty," *The Accounting Review* (83:3), pp 665-703.

Bergh, D.D. 1997. "Predicting Divestiture of Unrelated Acquisitions: An Integrative Model of Ex Ante Conditions," *Strategic Management Journal* (18:9), Oct, pp 715-731.

Bharadwaj, A.S. 2000. "A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation.," *MIS Quarterly* (24:1), 2000/03 p169.

Boehm, B. 1991. "Software Risk Management: Principles and Practices," *IEEE Software* (8:1), Jan, pp 32-41.

Booz.Allen.Hamilton. 2002. "Breaking up is Hard to Do - and to Manage," *strategy+business* (28).

Breslow, N. 1982. "Covariance Adjustment of Relative-Risk Estimates in Matched Studies," *Biometrics* (38:3), pp 661-672.

Broadbent, M., Weill, P., and St.Clair, D. 1999. "The Implications of Information Technology Infrastructure for Business Process Redesign.," *MIS Quarterly* (23:2), 1999/06 pp 159-182.

Brynjolfsson, E., Malone, T.W., Gurbaxani, V., and Kambil, A. 1994. "Does Information Technology Lead to Smaller Firms?," *Management Science* (40:12), pp 1628-1644.

Canada, J., Sutton, S.G., and Jr, J.R.K. 2009. "The Pervasive Nature of IT Controls: An Examination of Material Weaknesses in IT Controls and Audit Fees," *International Journal of Accounting and Information Management* (17:1), pp 106-119.

Cram, D.P., Karan, V., and Stuart, I. 2007. "Three Threats to Validity of Choice-Based and Matched Sample Studies in Accounting Research." Available at SSRN: http://ssrn.com/abstract=955031

Decker, C., and Mellewigt, T. 2007. "Thirty Years after Michael E. Porter: What Do We Know about Business Exit?," *Academy of Management Perspectives* (21:2), pp 41-55.

Deloitte. 2009. "A Closer Look at Carve-Outs." Retrieved July 11th, 2009, from http://www.deloitte.com/dtt/cda/doc/content/us_dcf_deloitte_divestiture_survey_report_190609.pdf

Doyle, J., Ge, W., and McVay, S. 2007. "Determinants of Weaknesses in Internal Control over Financial Reporting," *Journal of Accounting and Economics* (44:1-2), pp 193-223.

Ettredge, M.L., Chan, L., and Scholz, S. 2007. "Audit Fees and Auditor Dismissals in the Sarbanes-Oxley Era," *Accounting Horizons* (21:4), pp 371-386.

Gartner. 2005. "IT Handbook on Mergers, Acquisitions and Divestitures," *Gartner Research* (ID # G00130975), pp 1-65.

Grant, G.H., Miller, K.C., and Alali, F. 2008. "The Effect of IT Controls on Financial Reporting," *Managerial Auditing Journal* (23:8), pp 803-823.

Hammersley, J., Myers, L., and Shakespeare, C. 2008. "Market Reactions to the Disclosure of Internal Control Weaknesses and to the Characteristics of those Weaknesses under Section 302 of the Sarbanes Oxley Act of 2002," *Review of Accounting Studies* (13:1), pp 141-165.

Hosmer, D.W., and Lemeshow, S. 2004. *Applied Logistic Regression*, (2nd ed.). New York: Wiley.

IIA. 2005. *Global Technology Audit Guide (GTAG) 1: Information Technology Controls*. The Institute of Internal Auditors Research Foundation.

ITGI. 2006. *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control over Financial Reporting*, (2nd ed.). IT Governance Institute.

ITGI. 2007. *Cobit 4.1 Executive Summary and Framework*. IT Governance Institute

Kay, I.T., and Shelton, M. 2000. "The People Problem in Mergers," *The McKinsey Quarterly* (4), pp 27-37.

Kim, S.M., and Mahoney, J.T. 2006. "Mutual Commitment to Support Exchange: Relation-Specific IT System as a Substitute for Managerial Hierarchy," *Strategic Management Journal* (27:5), pp 401-423.

Kirsch, L.J. 2004. "Deploying Common Systems Globally: The Dynamics of Control," *Information Systems Research* (15:4), pp 374-395.

Lee, J.-N., Miranda, S.M., and Kim, Y.-M. 2004. "IT Outsourcing Strategies: Universalistic, Contingency, and Configurational Explanations of Success," *Information Systems Research* (15:2), pp 110-131.

Li, C., Lim, J.-H., and Wang, Q. 2007. "Internal and External Influences on IT Control Governance," *International Journal of Accounting Information Systems* (8:4), pp 225-239.

Lyytinen, K., Mathiassen, L., and Ropponen, J. 1998. "Attention Shaping and Software Risk - a Categorical Analysis of Four Classical Risk Management Approaches," *Information Systems Research* (9:3), pp 233-255.

Malhotra, A., Gosain, S., and El Sawy, O.A. 2007. "Leveraging Standard Electronic Business Interfaces to Enable Adaptive Supply Chain Partnerships," *Information Systems Research* (18:3), pp 260-279.

Mankins, M.C., Harding, D., and Weddigen, R.-M. 2008. "How the Best Divest," *Harvard Business Review* (86:10), pp 92-99.

Markus, M.L. 2000. "Paradigm Shifts—E-Business and Business / Systems Integration," *Communications of the Association for Information Systems* (4:10), pp 1-45.

Markus, M.L. 2001. "Reflections on the Systems Integration Enterprise," *Business Process Management Journal* (7:3), pp 1-9.

Mehta, M., and Hirschheim, R. 2007. "Strategic Alignment in Mergers and Acquisitions: Theorizing IS Integration Decision Making," *Journal of the Association for Information Systems* (8:3), pp 143-174.

Mookerjee, R. 2005. "Maintaining Enterprise Software Applications," *Communications of the ACM* (48:11), pp 75-79.

Ogneva, M., Subramanyam, K.R., and Raghunandan, K. 2007. "Internal Control Weakness and Cost of Equity: Evidence from SOX Section 404 Disclosures," *The Accounting Review* (82:5), pp 1255-1297.

Palepu, K. 1985. "Diversification Strategy, Profit Performance and the Entropy Measure," *Strategic Management Journal* (6:3), pp 239-255.

Parent, M., and Reich, B.H. 2009. "Governing Information Technology Risk," *California Management Review* (51:3), Spring, pp 134-152.

Parry, E. 2004. "SOX Wars: CIOs Share Ideas, Fears on Sarbanes-Oxley Compliance." Retrieved May 13th, 2009, from http://searchcio.techtarget.com/news/article/0,289142,sid182_gci994763,00.html

Perrow, C. 1999. *Normal Accidents: Living with High-Risk Technologies*, (updated ed.). Princeton, NJ: Princeton University Press.

Radhakrishnan, A., Zu, X., and Grover, V. 2008. "A Process-Oriented Perspective on Differential Business Value Creation by Information Technology: An Empirical Investigation," *Omega* (36:6), pp 1105-1125.

Raghunandan, K., and Rama, D.V. 2006. "SOX Section 404 Material Weakness Disclosures and Audit Fees," *Auditing: A Journal of Practice & Theory* (25:1), pp 99-114.

Rai, A., Patnayakuni, R., and Seth, N. 2006. "Firm Performance Impacts of Digitally-Enabled Supply Chain Integration Capabilities," *MIS Quarterly* (30:2), pp 225-246.

Rettig, C. 2007. "The Trouble with Enterprise Software," *MIT Sloan Management Review*. pp. 21-27.

Sabherwal, R., and Sabherwal, S. 2005. "Knowledge Management Using Information Technology: Determinants of Short-Term Impact on Firm Value," *Decision Sciences* (36:4), pp 531-567.

Sailpoint. 2009. "Minimizing Business Risk During a Merger, Acquisition or Divestiture." Retrieved July 22nd, 2009, from http://www.sailpoint.com/resources/files/webcast-030409/

Santhanam, R., and Hartono, E. 2003. "Issues in Linking Information Technology Capability to Firm Performance.," *MIS Quarterly* (27:1), 2003/03 p125.

Saraf, N., Langdon, C.S., and Gosain, S. 2007. "IS Application Capabilities and Relational Value in Interfirm Partnerships," *Information Systems Research* (18:3), Sep, pp 320-339.

Shimizu, K., and Hitt, M.A. 2005. "What Constrains or Facilitates Divestitures of Formerly Acquired Firms? The Effects of Organizational Inertia," *Journal of Management* (31:1), Feb, pp 50-72.

STATA. 2007. "20.15 Obtaining Robust Variance Estimates," in: *User's Guide, Release 10*. STATA Press.

Tanriverdi, H. 2005. "Information Technology Relatedness, Knowledge Management Capability, and Performance of Multibusiness Firms.," *MIS Quarterly* (29:2), Jun, pp 311-334.

Tanriverdi, H. 2006. "Performance Effects of Information Technology Synergies in Multibusiness Firms," *MIS Quarterly* (30:1), Mar, pp 57-77.

Tanriverdi, H., Konana, P., and Ge, L. 2007. "The Choice of Sourcing Mechanisms for Business Processes," *Information Systems Research* (18:3), Sep, pp 280-299.

Wade, M., and Hulland, J. 2004. "The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research," *MIS Quarterly*. pp. 107-142.

Zhang, Y., Zhou, J., and Zhou, N. 2007. "Audit Committee Quality, Auditor Independence, and Internal Control Weaknesses," *Journal of Accounting and Public Policy* (26:3), pp 300-327.