The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0268-6902.htm

Information intensity, control deficiency risk, and materiality

Akhilesh Chandra and Thomas G. Calderon
School of Accountancy, The University of Akron, Akron, Ohio, USA

Received 14 April 2008
Revised 31 August 2008
Accepted 9 September 2008

Abstract

Purpose – This paper leverages the concept of business information intensity (BII) with the aim of developing a model to assess control deficiency risk (CDR) in organizations. BII measures the extent of use of IT by an organization in its products and value chain.

Design/methodology/approach – The paper develops a conceptual model that uses BII and CDR to examine alternative approaches to risk management. This model contains four quadrants that provide insight into varying risk management strategies for business processes. CFOs and internal auditors from *Fortune* 100 companies are surveyed to illustrate how the model may be used to guide management in assessing IT security expenditure.

Findings – The model suggests that spending on IT and information security is higher for companies with high BII-CDR than those with low BII-CDR.

Research limitations/implications – Analysis focused on only two quadrants in a four-quadrant model. Future research may seek to refine the measurement of BII and CDR, and offer greater insight into the types of business processes that fall into each of the four quadrants as well as those that do not fit neatly into those quadrants.

Practical implications – Organizations may use the BII-CDR model to assess risk and to evaluate investments in IT security and other control activities. The model also highlights the need to redefine the concept of materiality and to consider its link to BII and CDR. Auditors should consider the interaction of BII and CDR in planning the audit, conducting field work, and managing overall audit risk.

Originality/value – The paper provides original insights into the relationship between BII and CDR and its implications for treatment of materiality. It was observed that activities which support critical business processes are themselves critical. This is an important departure from traditional approaches to evaluating materiality.

Keywords Information control, Data security, Risk management, Internal auditing

Paper type Research paper

Introduction

Current corporate governance regulations require companies with publicly traded securities to certify the existence, adequacy, and functionality of controls. Similar certification requirements are becoming more prevalent in non-public companies, as well as government and not-for-profit entities. The certification process relies on a model that emphasizes control deficiencies (Bell *et al.*, 2005). Control deficiencies by themselves are not necessarily damaging. However, a control deficiency may result in significant losses across the enterprise. Accordingly, we use the term control deficiency risk (CDR) to describe the likelihood that an organization will experience losses in the presence of loose, non-existent or ineffective controls. The potential financial loss defines the exposure attributable to a specific control deficiency in the organization.

Since IT is both an enabler of business processes and a driver of business strategy (Porter and Millar, 1985), it must feature extensively in any assessment of

Managerial Auditing Journal
Vol. 24 No. 3, 2009
pp. 220-232
© Emerald Group Publishing Limited
0268-6902
DOI 10.1108/02686900910941113

control deficiencies. In this context, we leverage the construct of business information intensity (BII) (Calderon *et al.*, 2001; Chandra and Calderon, 2003) and develop a model to help organizations assess control deficiencies. BII measures the usage of IT in an organization's products or value chain. Specifically, this paper has two goals: first, we theorize, by developing and discussing a model, the relationship between BII and CDR. Second, we surveyed CFOs' and internal auditors' to illustrate this relationship. Our results profile the characteristics and expenditure patterns for IT and IT security among companies with different combinations of BII and CDR.

The model highlights the need to redefine the concept of materiality and its link to control deficiencies. Specifically, a process-based approach to define materiality seems appropriate, and a key corollary of this approach is that activities, which support critical business processes, are themselves critical. This is an important departure from traditional approaches to evaluating materiality that focus on the monetary value of financial statement items. For example, FASB Concepts Statement No. 2, which provides a widely used definition of the concept, defines materiality as "the magnitude of an omission or misstatement of accounting information that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the omission or misstatement". Our process-based orientation of materiality evaluation increases focus, precision and objectivity and hence, also differs from the qualitative materiality advocated in the recent literature (Weinstein, 2007; Gist and Shastri, 2003; SAB, 99; SAS No., 107; ISA, 320; CON, 2). The model proposed in this paper also seeks to facilitate execution of the section 404 provision that requires management to identify the framework used to evaluate the internal controls (SOX, 2002).

Our model supported by an illustration could serve as a decision support resource for organizations that use IT extensively and must address internal control and corporate governance issues such as those mandated by the Sarbanes-Oxley Act. Management can use the model both in risk assessment during the certification process and in developing a corporate strategy to assess and manage risk. Finally, the model should help auditors to design audit programs for effectively managing audit risk and providing assurance on IT intensive business processes. Auditors are expected to assess both quantitative and qualitative aspects of materiality. A focus on only quantitative aspects of materiality can potentially increase audit risk as the auditor may ignore activities that are by themselves financially immaterial but may be necessary for substantively critical business processes.

The rest of the paper proceeds as follows: the next section describes and illustrates the concepts of BII and internal control deficiencies, and describes the BII-CDR model with implications for materiality; the third section examines companies' IT and IT security expenditure patterns in the context of a BII-CDR model; the fourth section discusses the implications for control and concludes the paper with a summary of findings and directions for future research.

Conceptual framework

Two essential components of the model are BII and internal control deficiencies. In this section, we develop the two constructs, relate them to assess materiality and suggest a measurement metric.

Business information intensity (BII)

Business processes of contemporary organizations are both facilitated by and embedded with IT. Any concept of BII should acknowledge the pervasiveness of IT in contemporary business processes. Consistent with the literature (Chandra and Calderon, 2005), we use BII to indicate the content and the extent of IT usage in an organization's products and value chain. An organization with high (low) IT content in its value chain, as well as its products, would have high (low) BII. BII can be modeled at both the product and business process levels. For example, both outsourcing and off-shoring business models present illustrations of activities that are potentially high in BII. Oracle provides an example of an organization that has outsourced its operations overseas. The overseas division and overseas business partners use IT to manage the outsourced operations. Further, overseas business partners leverage IT to create and transport the product back to Oracle's US-based headquarters. Thus, both the product and value chain are high in IT content and, therefore, high in BII.

Organizations also leverage IT to process, store, and exchange proprietary and sensitive information. The rapid proliferation of specific IT-enabled frameworks (e.g. web-enabled ERP systems and XML-based technologies) that allow companies to integrate their operations across the value chain has BII implications. For example, a financial institution can retrieve seamlessly and in real-time loan specific information from a client's publicly available SEC filings using a SOAP (simple object access protocol, which is a standard to exchange XML-based messages over computer networks) message and a web-service protocol. Similarly, a product design engineer in an overseas R&D facility can use XML standards to retrieve sensitive product specifications from the company's database. These illustrations represent organizations that have high BII in their business processes. In both these examples, the product is embedded with IT and the processes used in the value chain rely heavily on IT.

Control deficiency risk (CDR)

Integration of IT within and between business processes is a double-edged sword. The increased efficiency and effectiveness of IT to streamline business processes also exposes the same business processes to higher control deficiencies and vulnerabilities. IT tends to be vulnerable to several risks in such areas as confidentiality and privacy, availability of data and applications, and integrity of data and applications across distributed networks.

Control deficiencies increase the likelihood of loss to the organization by a threat. The threat could originate from an internal control weakness or from vulnerabilities in the internal control system that agents can exploit. The potential financial loss from a threat defines the exposure. For example, failure to secure access to information resources on laptops exposes organizations to significant potential losses each year. Stolen laptops from San Jose medical group contained private medical information on 185,000 people. Similarly, stolen laptops from UC Berkeley contained sensitive information on 98,000 graduate students (Roberts, 2005). Both examples could result in costly litigation, negative publicity, and out-of-pocket costs to correct the problem. Thus, control deficiencies are defined as the likelihood that an organization will experience losses in the presence of loose, non-existent or ineffective internal controls.

The nature of contemporary integrated information systems imply that the effect of any business transaction is felt instantly across the breadth and depth of the organization. The potential for cascading effects can be severely damaging if proper controls are not present or not fully operational.

Potential losses are significantly less when business processes are low in BII. An environment with low BII is characterized by a lack of integration across systems, constrained possibility of rapid propagation of an error across the enterprise, and delayed impact of an incident. These characteristics allow the organization to buy time in the event of an incident. Thus, the organization has better prospects to minimize damages and recover.

Changing concept of materiality

CDR is exacerbated in integrated, automated information systems with high BII. This is illustrated by the experience of a global conglomerate, which failed to pay a vendor's invoice that was classified as immaterial based on traditional thresholds. As a consequence, the company's website was shut down for an entire morning. The impact of this seemingly minor oversight by the company's accounts payable unit was felt instantly across several geographically disparate but inter-connected systems. The North American power outage of August 14, 2003 also highlights the realties of CDRs for integrated business processes with high BII. Similarly, the inability of Hershey (during 1999 Halloween and Thanksgiving holiday season) and Toys-R-Us (during 1999 Christmas season) to service their online orders consequent to glitches in their newly implemented SAP systems emphasizes the vulnerability of integrated systems to errors (Dugan, 1999).

Integrated systems are particularly vulnerable to seemingly immaterial events. These events cascade rapidly across the organization and its business partners. Thus, accountants and auditors should revisit the concept of materiality in an integrated enterprise with high BII. A seemingly immaterial oversight (e.g. failure to pay a small bill) in the context of a business process with high BII could cripple an organization. An important corollary of the BII concept is that every activity associated with a critical business process should be classified as critical. Each control weakness in a business process with high BII can translate into substantive financial exposure through an intentional exploitation of that weakness, or through simple error of omission or commission.

The process-based orientation of materiality differs from both the financial focus and subjective focus of materiality. The financial focus of the traditional approach (also called quantitative materiality) emphasizes a numerical threshold or rule-of-thumb to assess materiality. Such a threshold is typically anchored at a certain percentage or financial value of total expenses, revenues or earnings per share (Holstrum and Messier, 1982; Chewning *et al.*, 1989, 1998; Messier *et al.*, 2005). Any transaction or account value below the threshold is treated as immaterial.

Qualitative materiality (Jenkins, 2005) requires management, accountants and auditors to consider the full range of context and surrounding circumstances in assessing materiality. Such consideration may render a low financial value item as material. A holistic approach to materiality assessment is recommended by regulators (SAB, 99), standard setters (SAS, 107; ISA, 320; CON, 2), courts (re Citizens Utilities Co.;

re Kidder Peabody Securities Litigation, 1998; re Albert Glenn Yesner, 2001; re Dunlap, 2001), and prior research (Zabel and Benjamin, 2002; Ramos, 2004).

However, prior research has not provided a decision support to help assess either of the two materiality concepts (Messier, 1995). Further, most treatments of materiality are enumerated at the reporting and auditing stages. But the materiality concept is equally significant during collection and recording stages (CICA, 2005). The nature of materiality might differ between internal reporting and external reporting processes – the former is at operational level and detailed than the latter. Our model serves as a useful decision support for preparers, systems designers and auditors to assess materiality at data collection, recording, reporting and auditing stages. In the spirit of Jenkins (2005), the process approach requires managers, accountants, and auditors to evaluate the economic significance in assessing materiality.

BII-CDR model

The interaction of BII and CDR provides a valuable decision support for managers to streamline business operations, add value and achieve regulatory compliance. The decision support is reflected in Figure 1, which illustrates BII and CDR at varying levels of integrative detail along three dimensions – CDR, exposure and BII. The organizational profile object can be modified to reflect the BII, exposure and CDR characteristics of an organization. Thus, if the height of the object increases then the organization has a greater degree of CDR. If the width of the object expands then the organization has a higher level of exposure. Finally, the object could move to the left or right in relation to the BII axis depending on the degree of BII in the organization.

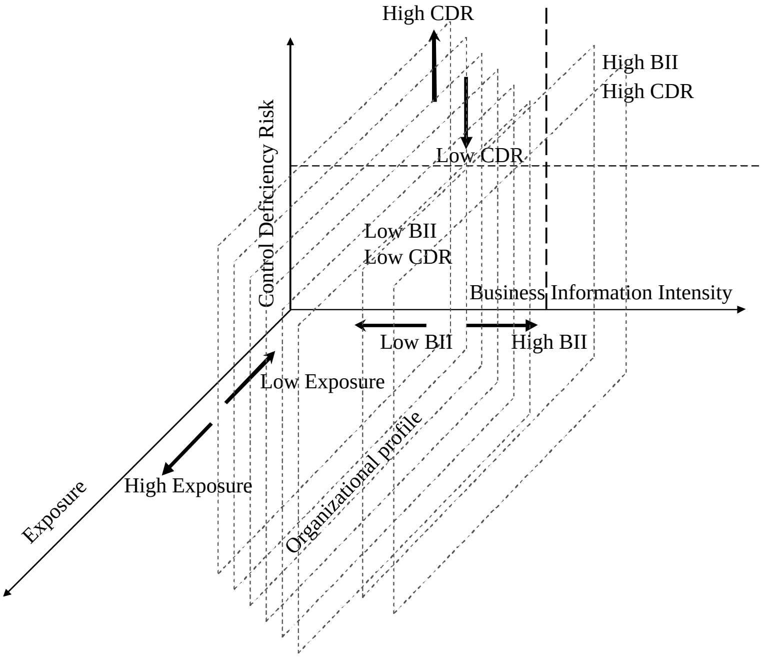


Figure 1.
Three-dimensional model for BII and CDRs

The interaction between BII, CDR and exposure can be associated with varying types of risk management strategies and security budgets in an organization. In a situation where exposure is low, a business process that falls in Quadrant IV (high BII – high CDR) may not justify a high level of expenditure to secure the process. Potential losses for the company would be low under those circumstances. However, it is clear that a process with high exposure and falls into Quadrant IV must be carefully protected, and higher levels of expenditure for security would be justified. In summary, this three way interaction calls for a measured response by organizations to manage both business risk and audit risks.

At the process level, different business processes of an organization will typically map to varying degrees of fit according to their BII and associated CDRs. At the entity level, managers can use the decision support to broadly categorize their divisions, operations or departments into varying levels of BII and CDR. At the product or functional level, Figure 1 can be used to address the adequacy of controls for managing risks for a certain level of BII.

For example, IT-based companies and the internet-based companies (such as Yahoo and Google) are generally high in BII (and can have potentially high CDRs). In comparison, pure brick and mortar operations are relatively low in both BII and CDR. A web-enabled data processing function for the purchasing or selling division of an organization provides an example of high BII at the department level. Should this department have vulnerable control systems, then it will have the potential for significant cascading losses. Transmission of daily medical records of patients' data for transcription by an outsourcing agency for a hospital illustrates a product-level classification that is high in BII with potentially high CDR. For example, if medical records are transmitted in clear-text then the organization is highly vulnerable to interception with potentially high exposure. CDR in such circumstances would certainly be high. A RFID enabled supply chain is an example of business process with high BII and the potential for high CDR. CDR is potentially high due to database connectivity issues and the inherent vulnerability of RFID systems (Rieback *et al.*, 2006). Weak access controls for database systems could allow an unauthorized entity to compromise data and jeopardize the integrity of RFID system.

Construct measurements

To serve as an effective decision support, the two constructs of the model should identify specific dimensions and a mechanism to measure and aggregate those dimensions. BII dimensions include the relative IT content in its products and services, value chain, information systems, and competitive strategies. CDR dimensions include control procedures, organizational and administrative processes, nature of organizational data, hierarchy, IT operations, and management of critical information infrastructure. The mechanism to aggregate various dimensions for each construct may vary across context and decision makers. We suggest one such variation that uses a rubric-based format to operationalize the two constructs. The basic framework for the rubric is depicted in Figure 2. To create a rubric, we make the following assumptions:

- Let X_{Bi} represent management's rating for component i in the BII construct within an organization.

- Let X_{Ej} represent management's rating for component j within the CDR construct.
- Let W_{Bi} represent a weight assigned by management to reflect the importance of surrogate component i within the context of BII.
- Let W_{Ej} represent a weight assigned by management to reflect the importance of surrogate component j within the context of CDR.

Based on these assumptions, we derive the following formulae for total BII and CDR scores:

- $\lambda = \sum (W_{Bi} X_{Bi})$, where λ represents the total BII score.
- $\varphi = \sum (W_{Ej} X_{Ej)}$, where φ represents the total CDR score.

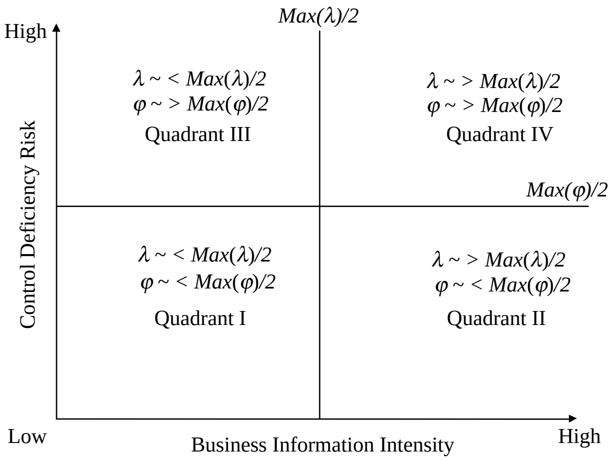
Both λ and φ will have known theoretical maximum values, as follows:

- $\mathrm{Max}(\lambda) = \sum [\mathrm{Max}(W_{Bi})^{*}\mathrm{Max}(X_{Bi})]$.
- $\mathrm{Max}(\varphi) = \sum[\mathrm{Max}(W_{Ej)}{}^{*}\ \mathrm{Max}(X_{Ej})]$.

Also, the theoretical minimum value will be zero since it is possible for BII to be insignificant and for CDR to be immaterial. This implies that the mid points for the BII and CDR axes can be defined as follows:

- Mid point of BII axis = $\mathrm{Max}(\lambda)/2$.
- Mid point of CDR axis = $\mathrm{Max}(\varphi)/2$.

Given these properties of the rubric, we provide the conceptual model in Figure 2 to classify business processes.



Notes: In this figure, λ, represents total BII score and φ, represents total CDR score. λ~ represents total computed BII score for a process and φ~ represents the total computed CDR score for a process

Figure 2.
A decision aid for using the access decision framework

This is a generalized model. Organizations that intend to use it must develop specific procedures and instruments to determine relevant weights and ratings for each process[1].

An example from the field

We conducted a cross-sectional study to understand the IT and security spending patterns of companies in various quadrants of the BII-CDR model. We used the BII-CDR model described in the previous section to assign companies in each quadrant based on a survey of *Fortune* 100 companies. We surveyed CFOs and internal auditors of *Fortune* 100 companies and received 72 usable responses. Each respondent was asked to assess BII and CDR for their respective organizations. Prior to mailing the final instrument, we pilot tested it among audit and finance professionals for completeness and clarity. We made changes to both the format and wording of the instrument based on the feedback received from the pilot.

We focus our discussion on Quadrants I and IV, which form the two extremes of the BII-CDR model. Focusing on the first and fourth quadrant allows us to highlight two categories of entities that should be substantively different. Our objective was to determine whether entities in the two extreme quadrants of the BII-CDR model demonstrate differences in their spending patterns for IT and IT security. Presumably, these two types of entities would have distinct spending patterns of IT and IT security as a result of their vastly different BII and CDR constructs.

Figure 3 shows the quadrants into which the sample of *Fortune* 100 companies fell. Although several companies do not group neatly into a unique quadrant, clusters that map into each of the four quadrants are evident. About 27 percent of the sample fell distinctly into Quadrant I, 20.8 percent fell into Quadrant II, 11 percent fell into Quadrant III, and 41 percent fell into Quadrant IV.

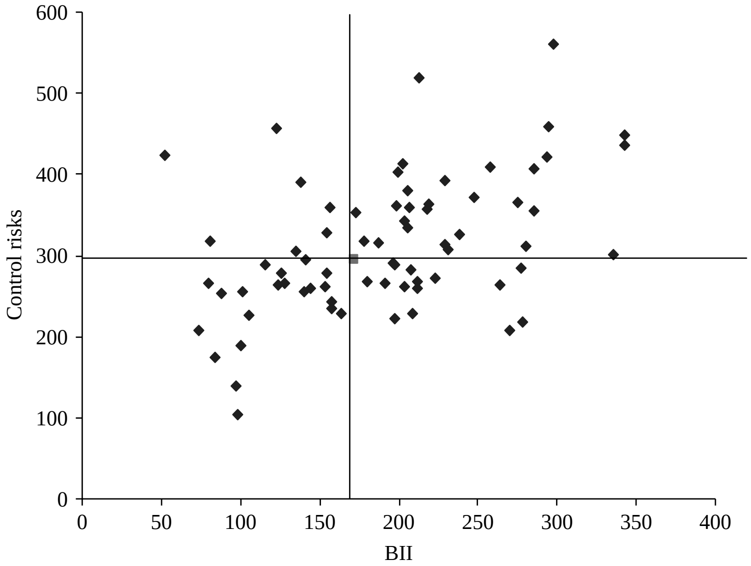


Figure 3.
Cluster of companies into respective quadrants

In considering the two extremes of the BII-CDR model, non-manufacturing firms constitute a higher proportion of the total sample within the high-BII-high-CDR category compared to the low BII-low CDR category (Table I). As a group, manufacturing firms represent the largest category in all quadrants.

Table II provides information on IT expense and IT security expense for the sample. We focus only on Quadrants I and IV in order to highlight the differences between various entities that fall into these two extreme quadrants. The differential nature of BII for manufacturing firms and total sample firms is evidenced by the mean annual expenditure on IT at the current and projected levels. Both manufacturing and total sample firms in Quadrant IV have higher average annual IT budgets compared with

	Industry	Number of firms	Proportion
Quadrant I	Manufacturing	9	45
	Insurance	2	10
	Government	1	5
	Other	8	40
Quadrant II	Manufacturing	6	40
	Consulting	2	13.3
	Insurance	1	6.7
	Other	6	40
Quadrant III	Manufacturing	3	37.5
	Consulting	1	12.5
	Insurance	1	12.5
	Banking	1	12.5
	Other	2	25
Quadrant IV	Manufacturing	7	24.1
	Consulting	3	10.3
	Insurance	5	17.2
	Government	3	10.3
	Banking	2	6.9
	Other	9	31.0

Table I.
Descriptive data

		Low BII-low CDR				High BII-high CDR		
		Quadrant 1				Quadrant 4		
	*	E1	E2	E3	*	E1	E2	E3
Full sample								
n	20	5	3	6	29	12	9	12
Mean		0.01	0.04	0.1		0.03	0.11	0.21
SD		0.01	0.05	0.05		0.02	0.15	0.27
Manufacturing								
n	9	4	2	4	7	4	2	5
Mean		0.01	0.01	0.08		0.04	0.05	0.28
SD		0.01	0	0.03		0.01	0.02	0.4

Notes: The table shows values for only those firms that provided data. Means and standard deviations are in percentage terms. *Indicates total firms within two extreme quadrants. E1, annual IT budget as a percent of sales; E2, annual IT budget as a percent of total expenses; E3, annual percent growth in IT security budget for the next three years; Quadrant 1, low BII-low CDR; and Quadrant 4, High BII-high CDR

Table II.
Trends in IT expenses and IT security expenses for the full sample and manufacturing firms

those in Quadrant I. The data shows a greater degree of variation in IT and IT security budgets among the high BII-CDR entities compared with their low BII-CDR counterparts. In essence, the combination of high BII and high CDR translates, as expected, to higher IT expenditures and IT security expenditures.

For the full sample of companies that provided data, annual IT budget as a percentage of sales, IT budget as a percentage of total expenses, and IT security growth are several times higher for Quadrant IV (high BII-high CDR) companies compared with Quadrant I (low BII-low CDR) companies. IT budget as a percentage of sales in Quadrant IV is three times the amount among Quadrant I companies; annual IT budget as a percentage of total expense is approximately three times higher; and percentage growth in IT security budgets is about twice as high. This pattern is mirrored when we analyze only manufacturing companies. In comparing across the two quadrants, it is evident that companies in Quadrant IV spend more on IT as well as IT security both as a percent of sales and total expenses. We interpret these observations to imply that, consistent with our expectations, low BII-low CDR companies invest less than high BII-high CDR companies in information technology and information security.

We should note that these results are only preliminary in nature. Our purpose in presenting these results is only to provide an illustration of the BII-CDR construct and not to test any specific hypothesis. Future extensions might examine the economic implications of the interaction between BII and CDR. In particular, researchers might examine the economic implications of processes that fall at or near the boundaries of any of the four quadrants. Similarly, researchers might also focus on the implications of alternative risk management strategies for processes that do not fall into well defined quadrants.

Limitations

Identification and measurement of BII is critical to precisely classify business processes or organizations into the four quadrants of our model. The instrument used in this study to measure BII is a good starting point. But companies use variations of these constructs to classify their business processes. Future research may focus on effective measurement of BII. Both theory and practice can also benefit from refining the instrument and methodology.

We reviewed two extreme cases – low BII and low CDR, and high BII and high CDR. Business processes in companies do not lend themselves to such neat and clear classification. Future studies should analyze business processes that overlap between quadrants for their implications for CDR. Also, the relative position of a business process or an entity within a specific quadrant may have implications for varying levels of CDR. In view of sample size constraints, our analysis uniformly treated all business processes in a quadrant as having identical implications regardless of their relative position within the quadrant. We also did not include company demographics in our review, and we did not intend to provide a comprehensive empirical test of the model.

We should note that these limitations do not reduce the significance of our model. The model relating BII and CDR provides a theoretical basis for future research and offers a framework for rethinking the concept of materiality.

Implications and conclusions

The BII-CDR model and the associated example have implications for selectively securing organizations' information infrastructure. Business processes with high BII and high CDR (high BII-CDR) need most protection and accordingly higher resource allocations. High levels of CDR may warrant a layered approach to information security with emphasis on defense-in-depth. Considering access controls, it is prudent to use multi-factor authentication systems in entities and business processes with high BII-high CDR.

The goals of confidentiality, integrity, and availability require a balance between protection, performance and access. Some of the new versions of intrusion detection systems and firewalls with multiple security checks may erode system performance and negatively affect user behavior. Business processes within the low BII-CDR category do not have high vulnerability and can be secured by less complicated security mechanisms.

Security for business processes between the two extremes – high BII-CDR and low BII-CDR – should be evaluated on an individual case basis. Significant factors in such decisions should consider the level of exposure, volume of transactions and cost of security and management. For example, individual identity-based verification and authentication may be unwarranted for a company to secure read-access to its financial statements and prospectuses that are already in the public domain. Making these documents available on the web is high in BII (due to the Internet based medium and IT based production process) but low in CDR (assuming that the statements are verified for accuracy and compliance with regulations).

The proposed decision support is useful for making trade-offs between IT investments and rigorous control mechanisms in designing secure information systems. Further, it is helpful for providing assurance on the quality and integrity of controls as greater levels of assurance would be needed for high BII-CDR processes relative to other processes. The interaction of BII and CDR should help managers mobilize the organization's resources to secure business processes that have the most impact on value creation and are most vulnerable. An understanding of the BII-CDR interplay could also help organizations make realistic forecasts and budget effectively for IT security. For example, organizations may budget more resources to protect processes and transactions with high BII-CDR. In contrast, smaller budgets would be justified for processes and transactions with low BII-CDR.

IT is a strategic factor in the current global economy. It alters the rules of competition, gives enterprises new ways to outperform competition, and forms the basis for creating new business models (Porter and Millar, 1985). However, use of IT may increase vulnerability and heighten CDR. The potential for elevated CDR varies as an increasing function of BII. Management should consider BII-CDR combinations to selectively secure their organization's vulnerable information resources in designing, monitoring, and evaluating information systems and other processes. In this context, management and accountants must revisit the concept of materiality and its link to CDR. An important implication of the BII-CDR model is that activities that support critical business processes are themselves critical. This is an important departure from traditional approaches to planning for materiality. Thus, auditors should consider the interaction of BII and CDR in planning the audit, conducting field work and managing overall audit risk.

Note

1. A possible instrument for capturing and operationalizing the BII and CDR constructs is available by contacting the authors at: tcalderon@uakron.edu or ac10@uakron.edu

References

Bell, T.B., Pecher, M.E. and Solomon, I. (2005), *The 21st Century Public Company Audit. Conceptual Elements of KPMG's Global Audit Methodology*, KPMG International, NJ.

Calderon, T.G., Sooduk, Seo and Il-Woon, Kim (2001), "An assessment of the contribution of information technology to financial performance: the case of commercial banks in Korea", *Journal of Applied Business Research*, Vol. 17 No. 2, pp. 83-96.

Chandra, A. and Calderon, T.G. (2003), "Toward a biometric security layer in accounting systems", *Journal of Information Systems*, Vol. 17 No. 2, pp. 51-70.

Chandra, A. and Calderon, T.G. (2005), "Challenges and constraints to the diffusion of biometrics in information systems", *Communications of the ACM.*, Vol. 48 No. 12, pp. 101-6.

Chewning, G., Pany, K. and Wheeler, S. (1989), "Auditor reporting decisions involving accounting principle changes: some evidence on materiality thresholds", *Journal of Accounting Research*, Vol. 27, Spring, pp. 78-96.

CICA (2005), *Handbook – Assurance (the Handbook)*, available at: www.aasb.ca/index.cfm/ci_id/7966/la_id/1.htm (accessed March 21, 2008).

CON 2 (Concepts Statement No. 2) (1980), *Qualitative Characteristics of Accounting Information*, FASB, Stamford, CT.

Dugan, S. (1999), "Why we owe our thanks to the Y2K problem", *InfoWorld*, December 29, available at: http://archives.cnn.com/1999/TECH/computing/12/29/owe.thanks.idg/index.html (accessed March 21, 2008).

Gist, W.E. and Shastri, T. (2003), "Revisiting materiality", available at: http://findarticles.com/p/articles/mi_qa5346/is_200311/ai_n21339301 (accessed March 21, 2008).

Holstrum, G.L. and Messier, W.F. (1982), "A review and integration of empirical research on materiality", *Auditing: A Journal of Practice & Theory*, Vol. 2 No. 4, pp. 45-63.

Jenkins, J.J. (2005), "The SEC's renewed embrace of qualitative materiality in enforcement proceedings", *The Corporate Governance Advisor*, September/October, pp. 22-9.

Messier, W.F. Jr (1995), "Research in and development of audit decision aids", in Ashton, R.H. and Ashton, A.H. (Eds), *Judgment and Decision-Making Research in Accounting and Auditing*, Cambridge University Press, NY.

Messier, W.F. Jr, Martinov-Bennie, N. and Eilifsen, A. (2005), "A review and integration of empirical research on materiality: two decades later", *Auditing: A Journal of Practice & Theory*, Vol. 24, pp. 153-87.

Porter, Michael E. and Millar, Victor A. (1985), "How information gives you competitive advantage", *Harvard Business Review*, Vol. 63 No. 4, pp. 149-74.

Ramos, M. (2004), "Section 404 compliance in the annual report", *Journal of Accountancy*, Vol. 21, available at: www.aicpa.org/PUBS/jofa/oct2004/ramos.htm (accessed March 21, 2008).

re Albert Glenn Yesner (2001), "Admin. Proc. File No. 3-9586", available at: www.sec.gov/litigation/aljdec/id184rgm.htm (accessed March 21, 2008).

re Dunlap (2001), *SEC v. Dunlap* et al., *01-8437-Civ-Dimitrouleas (S.D. Fla. Sept. 4)*, Zabel and Benjamin 2002.

re Kidder Peabody Securities Litigation (1998), "S.E.C. upholds ruling against ex-trader", March 8, 2004, available at: http://query.nytimes.com/gst/fullpage.html?res=9A0DE2D61F3FF93BA35750C0A9629C8B63 (accessed March 21, 2008).

Rieback, M.R., Crispo, B. and Tanenbaum, A.S. (2006), "Is your cat infected with a computer virus?", working paper, Vrije Universiteit Amsterdam, Computer Systems Group.

Roberts, P. (2005), "Stolen laptops contain medical info on 185,000 patients", *NetworkWorld*, IDG News Service 04/08/05, available at: www.networkworld.com/news/2005/0408stolelapto.html (accessed February 21, 2008).

SAB (1999), "SEC Staff Accounting Bulletin No. 99 – Materiality", available at: www.sec.gov/interps/account/sab99.htm (accessed March 21, 2008).

SAS 107 (2008), "Audit risk and materiality in conducting an audit", American Institute of Certified Public Accountants, available at: www.aicpa.org/download/members/div/auditstd/AU-00312.PDF (accessed March 21, 2008).

SOX (2002), "Pub.L. 107-204", Sarbanes-Oxley Act, available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname = 107_cong_public_laws&docid = f:publ204.107 (accessed March 21, 2008).

Weinstein, E.A. (2007), "Materiality: whose business is it?", *The CPA Journal*, Vol. 21, August, p. 2008, available at:www.nysscpa.org/cpajournal/2007/807/infocus/p24.htm (accessed March 21).

Zabel, R.B. and Benjamin, J.J. (2002), "Reviewing materiality in accounting fraud", *New York Law Journal*, Vol. 15, pp. 1-4.

Further reading

Porter, M.E. (1985), *Competitive Advantage*, The Free Press, NY.

About the authors

Akhilesh Chandra teaches in the area of accounting and information systems. His current research examines the impact of technology on the design and assurance issues of management control systems. Some of the journals in which his work is published includes *Communications of the ACM*, *Decision Support Systems*, and *Journal of Information Systems*.

Thomas G. Calderon is a past chair of the AAA's Teaching & Curriculum Section and past president of the AAA Ohio Region, he has published numerous academic and professional papers in auditing, information systems, and accounting education. His papers have appeared in *Auditing*, *Journal of Information Systems*, *International Journal of Accounting Information Systems*, *Advances in Accounting*, *Advances in Accounting Education*, *Issues in Accounting Education*, *Journal of Accounting Education*, *Managerial Auditing Journal*, *Communications of the ACM*, and many others. Thomas G. Calderon is the corresponding author and can be contacted at: tcalder@uakron.edu