Why do information system controls fail to prevent unethical behavior?

Karma Sherif
Department of Business Administration, Texas Southern University, Houston, Texas, USA, and
Richard Pitre and Mariatu Kamara
Department of Accounting and Finance, Texas Southern University, Houston, Texas, USA

Received 28 April 2015
Revised 20 December 2015
Accepted 25 February 2016

Abstract

Purpose – The purpose of this paper is to examine the ability of enterprise systems and embedded controls to prevent unethical behavior within organizations.

Design/methodology/approach – The authors use a case study to explore how the configuration of information technology (IT) controls within enterprise systems and their effectiveness in preventing unethical behavior is compromised by the tone at the top.

Findings – The study highlights the decisive role of cultural values and leadership in moderating the relationship between IT controls and unethical behavior and the realization that ethical environments are socially constructed not enforced.

Research limitations/implications – The limitation of this research is that the authors conducted one case study in an institution of higher education to refute the theory that IT controls embedded within enterprise systems can prevent unethical, and thus, the results may not be generalizable to other industries.

Practical implications – An important implication of the research is that the configuration of information system controls is affected by the organizational culture and the ethical values embraced by top management. When the tone at the top does not emphasize the ethical code of conduct, the configuration of IT controls will be compromised leaving organizations vulnerable at all levels.

Originality/value – Although the authors have a wealth of knowledge on ethics and theories that explain why unethical decision-making continue to surface to the headlines, they have little explanation as to why enterprise systems fail to stop unethical behavior in organizations. This study explores technical, organizational and individual factors that contribute to unethical decision-making.

Keywords Ethics, Enterprise resource planning, Case study methods, Configuration of the ERP system, IT controls, Tone at the top

Paper type Research paper

Given the recent corporate scandals that erupted in the past decade, there has been considerable interest in tools, processes and policies that prevent unethical behavior in organizations. Despite the wide adoption of information systems (IS) and the configuration of tight controls, it remains unclear why IS controls have not been successful in preventing unethical behavior. This research explores the impact of various detective and preventative IS controls on preventing unethical behavior. The

VINE Journal of Information and Knowledge Management Systems
Vol. 46 No. 2, 2016
pp. 251-266
© Emerald Group Publishing Limited
2059-5891
DOI 10.1108/VJIKMS-04-2015-0028

research also studies the effect of tone at the top in shaping ethical values and configuring IS controls. A case study approach is adopted, showing how an educational institution that adopted an expensive enterprise resource planning (ERP) system with a myriad of IS controls fails to stop unethical behavior at all levels until leadership is replaced and extensive training and dialogue begin to develop a new social identity. While qualitative evidence supports the ability of IS controls to limit unethical behavior, the study highlights the decisive role of cultural values and leadership in moderating the relationship. Findings also underscore the realization that ethical environments are socially constructed not enforced.

Introduction

The avalanche of recent corporate scandals triggered strong criticism of the exorbitant cost of unethical behavior to the public and to the business community as a whole (Dyck *et al.*, 2010). The public loss has sparked federal regulations, like the Sarbanes–Oxley Act of 2002 (SOX) and XBRL mandate (Dhole *et al.*, 2015), to enforce executive financial accountability and allow for comparison of financial statements across companies and industries. SOX and the XBRL force organizations to establish internal controls and proper documentation to ensure the integrity and accuracy of financial data (Li *et al.*, 2012). Major vendors of enterprise systems, like SAP and Oracle, have incorporated guidelines for internal controls into their design, attesting that built-in controls fully comply with federal requirements regarding data accessibility, validation of data entry and processing and storage of financial records (Morris, 2011).

IS controls are believed to equip organizations with the first line of defense to restrict unethical behavior (Morris, 2011), increasing the level of transparency and setting gatekeepers on the information and processes (Burns and Vaivo, 2001) to maintain the integrity of data and ensure the accuracy of financial reporting (Hsu *et al.*, 2006). Despite the attested rigor of IS controls (Morris, 2011), reported unethical behavior continues on the rise (PWC Report on Global Economic Crime, 2014), raising concerns on the viability of IS controls in restricting unethical behavior. It is not apparent if organizations are failing to properly configure IS controls or that technology by itself is insufficient to prevent unethical behavior. Studies assert that the long-term effect of configuration choices on accounting management control are unpredictable (Grabski *et al.*, 2011), and that leadership and ethical values are more important in defining the ethical environment of an organization than a set of controls embedded within systems (Ali *et al.*, 2009).

The success of IS controls in preventing unethical behavior is affected by an interplay of organizational context (Kallinikos, 2002; Granlund and Malmi, 2002), the human actors (Beaubien, 2013) and the technology design (Li *et al.*, 2012). Organizational culture, defined in the explicit code of conduct that leaders pass down to employees (Daft, 1992; Laczniak *et al.*, 1995), have a higher explanatory power as to why fraudulent activities continue to rise within organizations (Wood, 1995) than the adoption of IS controls and how they are configured. Leadership defines the cultural values for the whole organization (Nwachukwu and Vitell, 1997, Treviño *et al.*, 2003). They set the tone at the top that guides the daily behavior of individual members. Top management also appoints the information technology (IT) governance that defines and oversees the implementation of the IT strategy and ensures that the adopted technology is configured to support the ethical values upheld by top management (Zarvic *et al.*, 2012).

Top management is also responsible for setting up the internal and external audit entities that independently oversee the effectiveness and compliance of established IT controls with industry and federal regulations (Radnor, 1986). When top management, intentionally or unintentionally, neglect any of these responsibilities, they increase the risk of unethical behavior, where IS controls are bypassed (Granlund, 2001), ethics policies are absent (He and Ho, 2011), independent internal and external audits are weak (Dobler and Burt, 1996) and corporate culture is fraud-tolerant (Trevino and Victor, 1992).

This paper highlights the findings of a case study that examines how IS controls are circumvented when they are in conflict with the prevalent cultural values, allowing unethical behavior to flourish at all levels within an educational institution. When institutional efforts to reconstruct the culture and develop an ethical environment are undertaken, the configuring of IT controls to prevent unethical behavior becomes effective. The findings highlight the critical role top management and ethical values play to strengthen or weaken the effect of IS controls on unethical behavior. The study contributes to the literature of IS controls by establishing a framework to examine the interplay of IS, top management and ethical values in preventing unethical behavior.

Literature review and development of propositions

Unethical behavior is defined as behavior that is "either illegal or morally unacceptable to the larger community" (Jones, 1992, p. 367). This definition view ethics as a set of universal moral values that is common to all successful civilizations and that transcends differences in culture, ethnicity, age, religion and socio-economic status (Vitell and Davis, 1990). However, a close look at the causes of unethical behavior shows that in many organizational settings, the difference between ethical and unethical behavior is blurred (Nwachukwu and Vitell, 1997) and that decisions involving moral issues are complex and involve multiple normative frameworks to deal with value conflicts.

Organizations establish IS controls as a first line of defense against unethical behavior. The purpose of these controls is to maintain data integrity, and to detect and prevent unauthorized acquisition, use or disposition of the company's assets that could have a significant effect on the financial statements. At Level 1, controls authenticates user's rights and defines the roles and responsibilities of each employee to access data and functionality within the system (Siponen and Oinas-Kukkonen, 2007). The system enforces segregation of duties to prevent employees from assuming conflicting roles, like ordering and receiving, that can obscure fraudulent activities in the course of conducting daily business processes (Turner and Owhoso, 2009). At Level 2, controls establish a hierarchy of approvals where transactions are approved at different organizational levels before they are executed. Documents are cross-validated throughout a business cycle to ensure consistency. The system keeps a log of all actions taken within the system and prevents deletion or alterations to posted records. At Level 3, controls integrate data across distributed locations and consolidate reports across the enterprise (Li *et al.*, 2012). All three levels of IS controls are preventative controls that establish transparency and accountability (Schoenherr *et al.*, 2010). Post hoc detective controls are also provided collecting evidence through visualization of fraud detection (Dilla and Raschke, 2015), audit trails, analysis of variance, inspection of physical inventory and reconciliation of accounts, in case financial misconduct is successfully committed against the organization.

Despite stringent IS controls embedded within enterprise systems, a myriad of corporations in different industries have been entangled in allegations of fraudulent activities (Gray *et al.*, 2005). Among the most popular fraudulent scandals is the $7 billion case of the French multinational bank, Societe Generale, where one employee was able to circumvent robust IT security controls, creating fictitious accounts and falsified documents and manipulating funds in excess of $50 billion without being detected by IT system controls (Magee and Zaki, 2008). The fraud was only discovered when counter parties involved in the fraudulent trades alerted the bank (Magee and Zaki, 2008).

A recent review of the literature concludes that IS controls have had little impact on the practice of accounting management (Grabski *et al.*, 2011). In one study, IT controls were found to cause drift which results in a decrease in control (Ignatiadis and Nandhakumar, 2007). In the 2012 Association of Certified Fraud Examiners Report to the Nation, IT controls only detected 1.1 per cent of fraudulent activities compared to 43.3 per cent detected by tips and whistle-blowing (ACFE, 2012). One main problem with the ability of IS controls to limit fraud is its proper configuration (Turner and Owhoso, 2009). The way basic controls, like segregation of duties, are set up determine the effectiveness of the system (AICPA, 2001). Methodologies for assessing the information security control of financial statements has been proposed (Otero, 2015). Although proper configuration of IT controls can positively restrict unethical behavior, their effectiveness will depend on the cultural values upheld by top management.

The code of ethics that top management upholds is an important predictor of unethical behavior (Kaptein and Wempe, 1998; Nwachukwu and Vitell, 1997; Treviño *et al.*, 2003) and how IT controls are configured (Dong, 2008). While top management may not be technically competent to configure the system, the way they express their ethical values and articulate an ethics policy (Hunt and Jennings, 1997) affect the cultural norms that guide daily decision-making (Ferrell and Gresham, 1985; Kaptein, 2011) and how IT controls are configured. The vast majority of corporate fraud either show that top management directly benefited from the loose IT controls or they were "asleep at the switch" (AICPA) and failed to actively review the configuration of IT controls. Unethical behavior, thus, becomes the outcome of top management decisions rather than the problem of the aggressor. Holding top management legally responsible for financial fraud and encouraging the labor market to enforce that responsibility may solve the problem (Haislip *et al.*, 2015) (Figure 1).

Propositions

Based on the above discussion, we thus propose the following relationships:

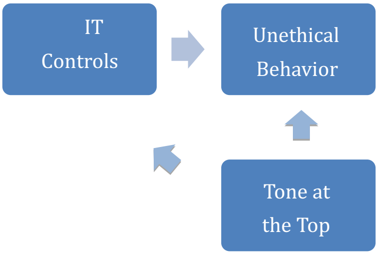

Figure 1.
The direct and indirect effect of tone at the top on IT controls and unethical behavior

P1. The proper configuration of IT controls will negatively impact unethical behavior within an organization.

P2. The tone at the top will affect how IT controls are configured.

P3. The tone at the top will affect the number of unethical behavior within an organization.

Research method

In this study, we adopted qualitative research as our methodological premise to explore the relationship between tone at the Top, IT controls and unethical behavior. Given the sensitive nature of the constructs we are studying, we chose to implement a longitudinal case study approach. We traded generalizability for the opportunity to observe the impact of IT controls on the development of an ethical work environment over a period of seven years from September 2007 to August 2014. The data were provided by informants in an urban university which, to preserve its anonymity, will be referred to as EDUCATOR. The research site was identified from the daily newspaper which reported financial scandals committed by the university's top administrators.

We interviewed 21 participants over a period of seven years: the current Chief Financial Officer (CFO), the former Chief Operating Officer, three Chief Information Officers, the former Vice President of IT, Directors of IT operations in the School of Business and the School of Law, a current IT manager in the administration building, three onsite IT consulting managers, four user liaisons and two ERP system administrators. Within the user community, we interviewed the Director and two IT specialists in the Office of Development. The questions were general open-ended questions to enable the participants to express freely their ideas without gauges from the research team as to what we consider important constructs:

Interview questions:

Q1. Please define your current role and daily responsibilities?

Q2. What kind of IS controls are set within the system? How were they configured?

Q3. Where you involved in setting up the controls?

Q4. In your opinion, how effective are the controls in preventing unethical behavior? Why were they ineffective during the previous administration?

Q5. Do you believe that IS controls are capable of creating an ethical environment?

Interviews took between 40-75 minutes. All interviews were transcribed except for one where extensive notes were taken.

Data analysis started with the transcription of the recorded interviews and categorizing statements under a concept suggested by the data, a process known as open coding. After all concepts were identified, a second coder, blind to the theoretical background for the study and the propositions suggested by the framework, went through the transcribed interviews and categorized the statements under identified codes. After several discussions of the coding scheme, inter-rate reliability between the two coders reached 85 per cent.

Concepts were further regrouped into one of the categories in our framework: tone at the top; IS controls; and unethical behavior. The process is known as selective coding. For example, segregation of duties, authorizations and tolerance limits were all grouped under IS controls. The final level of coding, theoretical coding, involved finding relationships between the codes in support of the propositions suggested by the framework. Examples of the coding process appear in Table I.

A write-up of the case after completing the data analysis enabled us to unfold in details why enterprise systems fail to prevent unethical behavior. The case highlighted how the tone at the top affected the configuration of the system and the prevalence of financial misconduct throughout the organization.

Findings

EDUCATOR is an institution of higher education with 9,500 student body, along with nearly 1,500 faculty and staff. At the beginning of the study, EDUCATOR was battling allegations of wrongdoing at different administrative levels after the President and the CFO were charged with unauthorized use of public funds. The main reason EDUCATOR failed to create an ethical environment is because of the relaxed attitude the former President revealed with regard to ethics and the message she sent to the rest of the institution. At the time the unethical behavior were committed, IT operations were outsourced to a large consulting firm, the developer of an enterprise system that is widely adopted by institutions of higher education. The main objective of the consulting firm was to guarantee a renewal of the contract by fulfilling all top management requests without much attention to industry standards or best practices in setting up the controls.

Information system controls

EDUCATOR's ERP system handled four main areas: procurement, financials, human resources and academics. It was up to the consulting firm to set up controls that would create a presumably ethical environment. According to the consulting firm's IT manager:

> The school was way behind the ball from the architecture standpoint. It was really hard to take advantage of the standards out there when there are foundational problems and no clear vision. we had to just consent to serving as the proxy leadership […] but there has never been an IT governance committee since we got here, no sort of an oversight or advisory or anything which is a bone of contention because that has left us on our own to determine what the priorities are […]. They are going to blame us for that. I don't think that was our responsibility.

The university admitted that there was no design of Business Process Integration to enforce security and close all of the loop holes within the system; however, they shoveled blame on the consulting firm:

> The vendor has not taken full responsibility for deploying this system properly because they depended upon the university. But the university hasn't the skill set. We are paying you x number of dollars, to do more than just act like a consultant; you can't sit back and just accept the money and not be capable or responsible for the end use of the product. So you should be driving that trend. As supposed to "well the administration told me not to". Well the administration know nothing about IT, they know you are just collecting a pay check.

The VP of technology, originally working for the consulting firm, did not see the importance of creating controls even within the IT department. Thus, IS controls were set at default values. There was no attempt to define roles and responsibilities that

Category	Concept	Excerpts
IT controls	Segregation of duties	In the past, the system analyst has been able to give certain individuals all the authority they requested without making sure they are aligned properly with the best practices. There are no checks and balances in place to make sure the authorizations are not in conflict
	Authorizations	We gave persons authority; instead of the position they assume. We should have realized that the role needs to have these types of accesses, not John because John may not be the CEO anymore
	Business rules	When setting up the systems, we did not have a business analyst who understands all of the business practices to make sure the business rules are set up within the system. As a result we had the paper system running side-by-side because we could not get full utilization
	Security	The security was not designed properly for it to work. We did not know exactly what we are giving each person. Now we design those securities based upon each person's applicable use of that system
	Tolerance limits	Clearly the electronic system is not forgiving. I would think the flexibility would be the primary one concern with the technology because there are some times when there's an exception, we have to figure out a way to deal with it, That makes it more complicating
Tone at the Top	Responsibility	There was no follow-up on decisions; no accountability for what went wrong. It was like this is our kingdom; we can do what we want
	loyalty	Loyalty was not to the university but to the President. She was surrounded by those who fully agreed with her all the time . . . the lunches, the bonuses and paid vacations made sure they remain loyal to her
	Integrity	There was no attempt to ensure that the people that work here come from an ethical background, having that basic ethical sense. . . We knew the CFO had criminal charges before but that did not stop him from being hired because he knew the President
Unethical behavior	Misuse of funds	The CFO approved purchases in excess of $1,000,000 for the President's residence, without getting the approval of the board
	Financial fraud	There were people on the payroll who were not working for the university, dependents covered by insurance who were not verified
	Financial negligence	When I first came on board, we found there were donation checks in people's desks written a year ago that were not deposited . . . we found three different types of software doing exactly the same thing and we were paying $750,000 a year

Table I. Concepts and categories for coding the data

ensure segregation of duties or set security rules to limit access to data and processes as related to responsibilities:

> Although the University had implemented a state of the art financial system, employees had not been trained on the utilization of the system and the corresponding controls. Access and responsibilities within the system were assigned to one employee giving that employee too much access. There were not adequate controls to ensure the integrity of the data. For example, the standards chart of accounts had not been adequately defined, nor maintained. Responsibility for the chart of accounts had moved between several offices and each time the coding of the chart of accounts had been done differently. As a result data could not be retrieved from the system with any consistency. Bank reconciliations had not been performed for more the 24 months.

In addition, some of the accounts were bundled in configuration to hide misuse of funds:

> […] it was intentionally set up this way, and I believe people who are entering the data on a daily basis are really aware that this is not the right way to do it.

There was no incentive to create an IT governance that aligns the alleged strategic goal of creating an ethical environment with the technological infrastructure. As a result, the tip of the balance kept shifting from a financially controlled environment to loosely held financial entities whose processes depended on administrators controlling financial resources within the different schools.

A new president took office two years after the start of the case study who held the position of CFO for a tier-one research institution. The President became known for his hands-on style of leadership, making sure he was involved in all major decisions across campus. Many of the administrative staff perceived his approach to be micromanaging and were thus replaced by new leadership.

After a new CFO was hired, IT controls were assessed:

> […] on a scale of 1 −10, 10 being a perfect environment, I gave the University a 2. I do not believe there was a university in the State, and likely not the Country, with worse controls at that time.

Major steps were taken to define IT controls within the ERP system to supplement the controls at the database level. At the very first level, user credentials determine the accessibility rights based on the role the user plays within an organization taking into consideration the segregation of duties and conflict of interests. A hierarchy of electronic authorizations was also established to ensure that proper approval has been granted for the use of school funds. The use of electronic approval improved lead time and closed all the gaps for approvals with no possibility of bypassing an authorization level. While employees complained of the rigidity and non-forgiving nature of the system, they agreed that the controls helped enforce the rules and regulations that the previous system frequently over-rode.

Another control established was the validation of data entered on financial documents. The system identifies certain fields as required and would not accept a document with missing fields. The financial documents are also cross-validated against other documents generated in a specific business cycle.

The system provided visibility for the use of funds across the institution. Individuals at different levels can view how appropriated funds have been expended and can check whether any violations have been committed. The system also generated summarized and detailed reports on the use of funds and traced all documents produced during a business cycle with the date and time of creation and the identity of the user responsible for the documented entry. Reports were generated with various options for slicing and dicing, rolling up and drilling down.

One of the challenges of configuring the system is the balance between flexibility and control. As a result of previous limitations, the new administration set rigid controls on internal business processes and a tight system of approval for code changes were in place. Employees complained the system was configured in an inflexible way that caused revolt among different operational staff. However, with criminal charges levied against some of the staff in the previous administration for failing to stop or report executive misuse of state funds, current staff believe the controls are a shield against executives' misuse of power and exercise of pressure on staff to collaborate on unethical behavior.

Despite the rigor of the IT controls, the new administration realized that no technology can fully safeguard an enterprise against unethical behavior, especially when the law does not fully cover the ethical spectrum. There can always be creative ways to override the system where the IS controls only make it challenging for someone set to commit fraud.

Unethical behavior

Several unethical behaviors surfaced during the interviews, starting with top management and trickling down through the organizational ladder. The former President and CFO were both charged with misuse of public funds. The values top management upheld trickled down the organizational ladder, leading to financial misconduct throughout the University. Employees were added to payroll without working for the university, and dependents were added to benefit who were not validated. Ethical problems stemmed from the lack of basic checks and balances that are normally set within the administrative structure. According to one administrative staff:

> […] because the same people who were doing the checks and balances are also the ones giving it approval […] People entering a proposal for funds were also the ones approving it making it difficult to detect unethical behavior.

There was also no backward tracking of business processes to enhance accountability. Databases were not linked to allow the assessment of major investments. There was an overall tendency set a low level of utilization of the functionality embedded within the ERP system to cover up for the rampant unethical behavior.

The tone at the top

The main reason informants attributed to the rampant financial misconduct across the institution was the relaxed attitude the former President revealed with regard to ethics and the message it sent to the rest of the institution. People working underneath the President also noted the loose control over the use of funds by the President's cabinet, and the frequent monetary rewards that the cabinet enjoyed during her tenure. With the President's moral standards relaxed, it was natural for those working underneath her to adopt the same standards.

Loyalty was first and foremost to the President that the Board's approval was bypassed for purchases in excess of $50,000. There was no questioning of the President's authority and no accountability for how funds were expended. Hiring of top executives was mainly based on the recommendations of the President. Interestingly, the Board of Regents failed to stop the financial misconduct and that students were the whistleblowers.

As the new President came to office, he realized the difficulty of changing the culture and unfreezing the cultural values in place and the bias that already existed to the status quo. The President undertook a substantial overhaul of leadership positions across the university. All personnel in the Office of the President were replaced along with the directors of Human Resource, Purchasing and operations. All deans and department heads were also replaced to facilitate setting a new tone at the top. The President emphasized the need for transparency at the top to build trust. At the beginning of each academic year, the President showcased his strict abidance to the rules, sharing reports of major operations and the financial status of the institution. The new administrative body was carefully restructured to ensure segregation of duties. The university also established strict policies and procedures for financial management and enforced mandatory training on ethical behavior for all those involved in handling monetary funds to instill a new mindset.

Implications of the study

Several studies have examined the impact of various organizational and individual factors on ethical decision-making. The role of IT controls in enforcing ethical behavior with respect to financial recording and reporting has not been fully examined. In this paper, we developed a model that proposes that the impact of IT controls on ethical behavior is mediated by the tone set by top management in the form of values upheld and the policies defined and enforced. We conducted a case study in an institution of higher education which adopted an ERP system, well-known for its internal controls. The case looks at the organization over a seven-year period and two presidents. The case is a classic example of what happens when there is a lack of willingness by top management to create a cultural organization based on ethical values such as honesty, respect, responsibility and compassion. Prior to the current administration, the ERP organization viewed ERP primarily as a means of processing data. The administration philosophy was to outsource the ERP function to enhance the processing of data. The former President and CFO of the institution were charged with financial fraud while the ERP system was operational. The question then arises as to why the IS controls in place did not stop fraudulent acts. When the current administration assumed office a cultural shift occurred. This cultural shift created a baseline starting point to define the different aspects of what is tone at the top (Verschoor, 1998). The first step of the baseline was to view ERP as an integral part of the management process. It returned the ERP function in-house viewing it as the linchpin of the organization's internal control environment. An important realization of the case is that the configuration of IS controls is affected by the ethical values embraced by top management. This philosophy contributes to the integrity of the financial reporting process. It is vital if fraudulent financial reporting is to be controlled. When the tone at the top does not emphasize the importance of following an ethical code of conduct, the controls are bypassed and the organization is left vulnerable at all levels. When the administration is replaced with more ethically driven leadership, the organization relearns a new set of beliefs and iteratively develops the moral character (Kohlberg, 1973). It is impossible for an IS to fully develop a cognitively moral environment. The system can provide transparency and build accountability for actions taken within the system. However, there is no attempt to change an employee's reasoning and moral judgment of what is good for the organization and the society as a whole. In fact, with a corrupt top management, the system can be loosely configured to where basic understanding of what is unethical may not be attainable. The tone at the top is a critical determinant of how ethical the environment will be. When top management takes a relaxed attitude towards the handling of funds, responsibility and accountability and nurture loyalty to individuals versus the institution, the environment becomes prone to committing unethical behavior. It is the role of internal audits to assess the tone of the top and take an active role in configuring the ERP system to reduce the risk of fraud (Tsai and Chou, 2015). The proper configuration of the ERP would allow auditors to monitor transaction processes, investigate fraud claims and examine data integrity. When internal audits fail to assess the tone at the top and ignore their role in identifying and rectifying control weaknesses in an ERP system, they set the stage for the advent of fraud (Tsai and Chou, 2015). Special attention is needed to train internal auditors to asses the tone at the top, as research found that auditors disregard management intentions when judging fraud cases (Jamal *et al.*, 2015).

For organizations to develop a moral identity, executives need to transparently show that they strictly follow the code of conduct they set within the ethics policy (Bourass, 2014). The integrated approach of setting rigorous IT controls and having ethical leadership will help organizations evolve from the pre-conventional stage of moral development where individuals acknowledge the norms of ethical behavior to the principled stage where decision makers at all levels within the organization exhibit ethical sensitivity and develop a social consensus on what constitute unethical behavior (Beu and Buckley, 2001; May and Pauli, 2002).

Conclusion

While we have a wealth of knowledge on ethics and theories that explain why unethical decision-making continues to surface to the headlines, we have little explanation as to why enterprise systems fail to stop unethical behavior. This study explores the effect of the tone at the top in weakening the effect of IT controls in preventing unethical behavior. While IT controls are capable of preventing misuse of funds, they are deficient by themselves to create an ethical environment (Brandas *et al.*, 2013). Organizations need to set the right tone at the top to build a culture where ethical decision-making is second nature.

A few limitations of this study should be noted. First, the study is based on a single case, limiting the ability to generalize the results across industries and across different company size. Future research should investigate the effect of ERP systems on fraudulent activities in companies that differ in size, industry and ERP solutions implemented. In addition, we believe that the scope of implementation and the level of integration of the financial module with other modules will impact the effectiveness of the system and its resilience in creating an ethical environment.

References

Ali, S., Green, P. and Parent, M. (2009), "The role of a culture of compliance in information technology governance", in Sadiq, S., Indulska, M. and Muehlen, M. (Eds), *2nd International Workshop on Governance, Risk and Compliance (GRCIS 09)*, Amsterdam, Netherlands.

Arnott, R. (2004), "Ethics and unintended consequences", *Financial Analysts Journal*, Vol. 60 No. 3, pp. 6-8.

Beaubien, L. (2013), "Technology, change, and management control: a temporal perspective", *Accounting, Auditing & Accountability Journal*, Vol. 26 No. 1, pp. 48-74.

Beu, D. and Buckley, M.R. (2001), "The hypothesized relationship between accountability and ethical behavior", *Journal of Business Ethics*, Vol. 34 No. 1.

Bourass, Y. (2014), "The role of the firms governance bodies in the fight against fraud-case of the board of directors", *International Journal of Management Sciences and Business Research*, Vol. 3 No. 10, pp. 12-15.

Brandas, C., Stirbu, D. and Didraga, O. (2013), "Integrated approach model of risk, control and auditing of accounting information systems", *Informatica Economica*, Vol. 17 No. 4, pp. 87-95.

Burns, J. and Vaivo, J. (2001), "Management accounting change", *Management Accounting Research*, Vol. 12 No. 4, pp. 389-402.

Daft, R.L. (1992), *Organizational Theory and Design*, West Publishing, St Paul, MN.

Dhole, S., Lobo, G., Mishra, S. and Pal, A. (2015), "Effects of the SEC's XBRL mandate on financial reporting comparability", *International Journal of Accounting Information Systems*, Vol. 19 No. 1, pp. 29-44.

Dilla, W. and Raschke, R. (2015), "Data visualization for fraud detection: practice implications and a call for future research", *International Journal of Accounting Information Systems*, Vol. 16 No. 1, pp. 1-22.

Dobler, D.W. and Burt, D.N. (1996), *Purchasing and Supply Management: Text and Cases*, 6th ed., McGraw-Hill, New York.

Dong, L. (2008), "Exploring the impact of top management support of enterprise systems implementations outcomes", *Business Process Management Journal*, Vol. 14 No. 2, pp. 204-218.

Dyck, A., Morse, A. and Zingales, L. (2010), "Who blows the whistle on corporate fraud?", *Journal of Finance*, Vol. 65 No. 6, pp. 2213-2253.

Ferrell, O.C. and Gresham, L.G. (1985), "A contingency framework for understanding ethical decision making in marketing", *Journal of Marketing*, Vol. 49 No. 3, p. 87, available at: http://0-search.proquest.com.mylibrary.qu.edu.qa/docview/227737133?accountid=13370

Grabski, S.V., Leech, S.A. and Schmidt, P.J. (2011), "A review of ERP research: a future agenda for accounting information systems", *Journal of Information Systems*, Vol. 25 No. 1, pp. 37-78.

Granlund, M. (2001), "Towards explaining stability in and around management accounting systems", *Management Accounting Research*, Vol. 12 No. 2, pp. 141-166.

Granlund, M. and Malmi, T. (2002), "Moderate impact of ERPS on management accounting: a lag or permanent outcome?", *Management Accounting Research*, Vol. 13 No. 3, pp. 299-321.

Gray, K.R., Larry, A.F. and George, W.C. (2005), *Corporate Scandals: The Many Faces of Greed*, Paragon House, St. Paul, MN.

Haislip, J., Masli, A., Richardson, V. and Watson, M. (2015), "External reputational penalties for CEOs and CFOs following information technology material weaknesses", *International Journal of Accounting Information Systems*, Vol. 17 No. 1, pp. 1-15.

He, L. and Ho, S.K. (2011), "Monitoring costs, managerial ethics and corporate governance: a modeling approach", *Journal of Business Ethics*, Vol. 99 No. 4, pp. 623-635.

Hsu, K., Sylvestre, J. and Sayed, E.N. (2006), "Avoiding ERP pitfalls", *Journal of Corporate Accounting & Finance*, Vol. 17 No. 4, pp. 67-74.

Hunt, T.G. and Jennings, D.F. (1997), "Ethics and performance: a simulation analysis of team decision making", *Journal of Business Ethics*, Vol. 16 No. 2, pp. 195-203, available at: http://0-search.proquest.com.mylibrary.qu.edu.qa/docview/198089265?accountid=13370

Ignatiadis, I. and Nandhakumar, J. (2007), "The impact of enterprise systems on organizational control and drift: a human-machine agency perspective", *International Journal of Enterprise Information Systems*, Vol. 3 No. 3, pp. 36-39, pp. 41-51.

Jamal, K., Chen, H. and Luo, L. (2015), "Are evaluations of audit quality influenced by management's intentions and outcomes?", *Asia – Pacific Journal of Accounting & Economics: APJAE*, Vol. 22 No. 2, p. 191.

Jones, T. (1992), "Ethical decision making by individuals in organizations: an issue contingent model", *Academy of Management Review*, Vol. 16 No. 2, pp. 366-395.

Kallinikos, J. (2002), "Reopening the black box of technology artifacts and human agency", *ICIS 2002 Proceedings*, Paper 26, available at: http://aisel.aisnet.org/icis2002/26

Kaptein, M. (2011), "From inaction to external whistleblowing: the influence of the ethical culture of organizations on employee responses to observed wrongdoing", *Journal of Business Ethics*, Vol. 98 No. 3, pp. 513-530. doi: http://0-dx.doi.org.mylibrary.qu.edu.qa/10.1007/s10551-010-0591-1.

Kaptein, M. and Wempe, J. (1998), "Twelve Gordian knots when developing an organizational code of ethics", *Journal of Business Ethics*, Vol. 17 No. 8, pp. 853-869.

Kohlberg, L. (1973), "The claim to moral adequacy of a highest stage of moral judgement", *Journal of Philosophy*, Vol. 70, pp. 630-646, available at: http://dx.doi.org/10.2307/2025030

Krishnan, G.V. and Visvanathan, G. (2007), "Reporting internal control deficiencies in the post-Sarbanes-Oxley era: the role of auditors and corporate governance", *International Journal of Auditing*, Vol. 11 No. 2, pp. 73-90.

Laczniak, G.R., Berkowitz, M.W., Brooker, R.G. and Hale, J.P. (1995), "The ethics of business: improving or deteriorating?", *Business Horizons*, Vol. 38 No. 1, pp. 39-47.

Li, C., Peters, G.F., Richardson, V.J. and Weidenmier Watson, M. (2012), "The consequences of information technology control weaknesses on management information systems: the case of sarbanes-Oxley internal control reports", *MIS Quarterly*, Vol. 36 No. 1, pp. 179-204.

Magee, J.C. and Zaki, S. (2008), "Preventing fraud losses through real-time risk monitoring", available at: www.corporatecomplianceinsights.com/wp-content/uploads/gravity_forms/14-f3c6012ed7b64af70e209c6db8553b08/2012/01/WP_Societe_Generale-v3-13-032708-jm.pdf

May, D.R. and Pauli, K.P. (2002), "Ethics and the digital dragnet: magnitude of consequences, accountability, and the ethical decision making of information systems professionals" *Best Paper Electronic Proceedings of the Academy of Management, Denver, CO*.

Morris, J.J. (2011), "The impact of Enterprise Resource Planning (ERP) systems on the effectiveness of internal controls over financial reporting", *Journal of Information Systems*, Vol. 25 No. 1, pp. 129-157.

Nwachukwu, S. and Vitell, S. (1997), "The influence of corporate culture on managerial ethical judgments", *Journal of Business Ethics*, Vol. 16 No. 8, pp. 757-776.

Otero, A. (2015), "An information security control assessment methodology for organizations' financial information", *International Journal of Accounting Information System*, Vol. 18 No. 1, pp. 26-25.

PWC Report on Global Economic Crime (2014), available at: www.pwc.com/gx/en/economic-crime-survey/

Radnor, M. (1986), "Technology strategy: internal and external perspectives", *International Journal of Technology Management*, Vol. 1 No. 3, p. 502.

Schoenherr, T., Hilpert, D., Soni, A.K., Venkataramanan, M.A. and Mabert, V.A. (2010), "Enterprise systems complexity and its antecedents: a grounded-theory approach", *International Journal of Operations & Production Management*, Vol. 30 No. 6, pp. 639-668.

Siponen, M. and Oinas-Kukkonen, H. (2007), "A review of information security issues and respective research contributions", *Data Base for Advances in Information Systems*, Vol. 38 No. 1, pp. 60-80.

The Association of Certified Fraud Examiners (ACFE) (2012), *Report to The Nation*, available at: www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

Trevino, L.K. and Victor, B. (1992), "Peer reporting of unethical behavior: a social context perspective", *Academy of Management Journal*, 35, 38-64.

Treviño, L., Brown, M. and Hartman, L. (2003), "A qualitative investigation of perceived executive ethical leadership: perceptions from inside and outside the executive suite", *Human Relations*, Vol. 56 No. 1, p. 5.

Tsai, B. and Chou, S. (2015), "Application of multiple output data envelopment analysis in interpreting efficiency improvement of enterprise resource planning in integrated circuit firms", *The Journal of Developing Areas*, Vol. 49 No. 1, pp. 285-304, available at: http://0search.proquest.com.mylibrary.qu.edu.qa/docview/1620439608?accountid=13370

Turner, L.D. and Owhoso, V. (2009), "Use ERP internal control exception reports to monitor and improve controls", *Management Accounting Quarterly*, Vol. 10 No. 3, pp. 41-50.

Verschoor, C. (1998), "A study of the link between a corporation's financial performance and its commitment to ethics", *Journal of Business Ethics*, Vol. 17 No. 13, pp. 1509-1516.

Vitell, S. and Davis, D. (1990), "Ethical beliefs of MIS professionals: the frequency and opportunity for unethical behavior", *Journal of Business Ethics*, Vol. 9 No. 1, pp. 63-70.

Volonino, L., Gessner, G.H. and Kermis, G.F. (2004), "Holistic compliance with Sarbanes-Oxley", *Communications of the Association for Information Systems*, Vol. 14 No. 1, p. 1.

Wood, G. (1995), "Ethics at the purchasing/sales interface: an international perspective", *International Marketing Review*, Vol. 12 No. 4, pp. 7-19.

Zarvic, N., Stolze, C., Boehm, M. and Thomas, O. (2012), "Dependency-based IT governance practices in inter-organisational collaborations: a graph-driven elaboration", *International Journal of Information Management*, Vol. 32 No. 6, p. 541.

Further reading

American Institute of Certified Public Accountants (AICPA) (2001), *The Effect of Information Technology on the Auditors' Consideration of Internal Control in a Financial Statement Audit*, SAS No. 94, AICPA, New York, NY.

Barnett, T. and Valentine, S. (2004), "Issue contingencies and marketers' recognition of ethical issues, ethical judgments and behavioral intentions", *Journal of Business Research*, Vol. 57 No. 4, pp. 338-346.

Carter, C.R. (2000), "Precursors of unethical behavior in global supplier management", *Journal of Supply Chain Management*, Vol. 36 No. 1, pp. 45-56.

Chang, S., Yen, D.C., Chang, I. and Jan, D. (2014), "Internal control framework for a compliant ERP system", *Information & Management*, Vol. 51 No. 2, p. 187.

Collins, J. (2009), *How the Mighty Fall and Why Some Companies Never Give in*, Harper Collins Publishers, New York.

Dell, S., Rollins, K.B., Schneider, J.M., Jackson, M.L. and Dunning, N.A.R. (2010), US Securities and Exchange Commission Civil action no 1: 10-CV-01245 (D.D.C.).

George, N. (2012), "Financial statement fraud and corporate governance", *Review of Business Research*, Vol. 12 No. 3, pp. 34-43.

Hunt, S.D. and Vitell, S.J. (1986), "A general theory of marketing ethics", *Journal of Macromarketing*, Vol. 6 No. 1, p. 5.

IT Governance Institute (2006), *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting*, Information Systems Audit and Control Association (ISACA).

Knutsen, O. (1995), "Value orientations, political conflicts and left-right identification: a comparative study", *European Journal of Political Research*, Vol. 28 No. 1, pp. 63-93.

Liu, A.Z. and Seddon, P. (2009), "Understanding how project critical success factors affect organizational benefits from enterprise systems", *Business Process Management Journal*, Vol. 15 No. 5, pp. 716-743.

Lorenzo, O. (2004), "A comprehensive review of the enterprise systems research", Instituto de Empresa Business School Working Paper No WP, Vol. 12 No. 4, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1003752

Melin, U. (2010), "The enterprise system as a part of an organization's administrative paradox", *Journal of Information Management*, Vol. 23 No. 2, pp. 181-200.

Miceli, J.P., Marcia, P.N. and Terry, M.D. (2009), "Wrong doing", *Journal*, Vol. 86 No. 3, pp. 379-396.

Parboteeah, K.P. and Cullen, J.B. (2002), "Justifications to commit unethical behaviors among managers: a social institutions approach", Paper presented and selected as Conference Best Papers at the 2002 Academy of Management Meetings in Denver, CO. Included in proceedings.

Pierce, L. and Snyder, J. (2008), "Ethical spillovers in firms: evidence from vehicle emissions testing", *Management Science*, Vol. 54 No. 11, pp. 1891-1903.

Robey, D., Ross, J.W. and Boudreau, M.C. (2002), "Learning to implement enterprise systems: an exploratory study of the dialectics of change", *Journal of Management Information Systems*, Vol. 19 No. 1, pp. 17-46.

Rotter, J. (1966), "Generalized expectancies for internal vs external control of reinforcements", *Psychological Monographs*, Vol. 80 No. 1.

Schwartz, M., Dunfee, T. and Kline, M. (2005), "Tone at the top: an ethics code for directors?", *Journal of Business Ethics*, Vol. 58 Nos 1/3, pp. 79-100.

Schwarzer, R. (1992), *Self-efficacy: Thought Control of Action*, Taylor and Francis, Routledge, London.

SEC (2009), *Study of the Sarbanes-Oxley Act of 2002 Section 404 Internal Control over Financial Reporting Requirements*, available at: www.sec.gov/news/studies/2009/sox-404_study.pdf

Stephens, N.M. (2011), "External auditor characteristics and internal control reporting under SOX section 302", *Managerial Auditing Journal*, Vol. 26 No. 2, pp. 114-129.

Strong, J.M., Portz, K. and Busta, B. (2006), "A first look at the accounting information system emphasis at one university: an exploratory analysis", *The Review of Business Information Systems*, Vol. 10 No. 2, pp. 29-39.

Thomas, J.R., Schermerhorn, J. and John, W.D. (2004), "Strategic leadership of ethical behavior in business", *Academy of Management Executive*, Vol. 18 No. 2.

Trevino, L.K. and Brown, M. (2004), "Managing to be ethical: debunking five business ethics myth", *Academy of Management Executive*, Vol. 18, 69-81.

Trevino, L.K. and Youngblood, S.A. (1990), "Bad Apples in Bad Barrels: a causal analysis of ethical decision making behavior", *Journal of Applied Psychology*, Vol. 75 No. 4, pp. 378-385.

US Securities and Exchange Commission (2010), "US Securities and Exchange Commission, Litigation Release No. 21599 (July 22, 2010)", available at: www.sec.gov/litigation/litreleases/2010/lr21599.htm

Corresponding author
Karma Sherif can be contacted at: sherifk@tsu.edu