IT GOVERNANCE FRAMEWORK: ONE SIZE FITS ALL?

Full Papers

Hwee-Joo Kam
Ferris State University
kamh@ferris.edu

Pairin Katerattanakul
Western Michigan University
p.katerattanakul@wmich.edu

SoonGoo Hong
Dong-A University
shong@daunet.donga.ac.kr

Abstract

Most of the IT governance frameworks address information systems management in the corporate settings that support top-down management. However, this neglects some organizational settings in favor of bottom-up approach, such as, higher education. To close the gap, this study compares the management styles and organizational practices between higher education and banking industry to reveal the underlying factors that drive organizational security norms in both industries. The results reveal that higher education operates in an open environment that supports employee's participation for policy compliance. On the other hand, top-down management enforces policies and facilitates employee's participation for information security safeguard in the banking industry. Accordingly, this study suggests that a new paradigm of IT Governance framework (ITG) is necessary for addressing the unique culture of higher education. Additionally, IT governance can operate in a decentralized mode in the banking industry for encouraging employee's participation in support of information policy compliance.

Keywords:

IT governance, banking industry, higher education

Introduction

Top-down management has been advocated as an effective way to enforce information security policy (ISP) (Hu, Dinev Hart and Cooke 2012). Organizations adopt top-down management along with IT governance framework (ITG) to comply with information security regulations. For example, banking organizations, defined by hierarchical culture (Claessens 2012) in support of top-down management, employ COBIT framework for auditing (Panopoulos 2012) and Sarbanes-Oxley (SOX) compliant (Barve n.d.). COBIT, stands for Control Objectives for Information and related Technology, represents an IT governance framework (ITG) that integrates and institutionalizes good practices to ensure that the enterprise's IT supports business objectives. Overall, IT governance entails authority for key IT activities in organizations, including IT infrastructure, IT application and project management (Sambamurthy and Zmud, 1999). Most of the guidelines suggested in ITG are tailored to corporate settings that practice top-down management (Yanosky and McCredie 2008).

However, there are some organizational settings that support bottom-up management. For example, in higher education, the "bottom-up" approach gives some decision-making power to faculty members (Reis 1997). In the United States, universities and colleges begin to integrate IT governance framework into higher education settings (Grama 2015). IT governance guides higher education to attain regulatory compliance (Stiles 2012) when higher education is facing higher scrutiny from the public (Yanosky and Caruso 2008). Nevertheless, IT governance frameworks do not address the unique culture of higher education. In specific, Yanosky and McCredie (2008) stated that:

"Higher education IT leaders will quickly note, however, that existing ITG models are largely based on corporate practice, and that they may assume organizational hierarchies, or identify performance goals, that don't map directly to such higher education realities…." (pg. 23)

In short, there is no one-size-fits-all approach in IT governance. To address this shortcoming, this study examines two industries, namely, banking and higher education, to provide viable suggestions on how to align IT governance with different management styles when *"one size does not indeed fit all"*. Particularly, in the context of information security, this study investigates how differences in management and organizational practices generate differences in organizational security norms across industries. The findings will then enable us to suggest viable approaches that empower organizations to effectively implement IT governance in multiple organizational settings for improving information security safeguard. Hence, the research questions are:

RQ1: How do management and organizational practices drive higher education and banking industry to shape organizational security norms?

RQ2: How to align IT Governance Framework (ITG) with organizational practices for enhancing information security?

This study selects higher education and banking industry for one main reason. In general, we argue that higher education and banking industry have a different set of organizational cultures and stakeholder's expectation for information security safeguards. Accordingly, this leads to different management styles and organizational practices. By making a cross comparison between both industries, this study is able to examine the effectiveness of information security policies (ISP) enforcement versus employee's participation in shaping organizational security norms. Mainly, hierarchical culture in banks supports top-down management (Claessens 2012) for ISP enforcement. On the other hand, as most universities and colleges embrace participatory leadership (Gilmour 1991) and shared governance (Yanosky and McCredie 2008) that involves employees in decision making (Yukl and Becker 2006), employee's participation in decision making for ISP might be more applicable in higher education. Thus, comparing and contrasting employee's participation that empowers employees (Yukl and Becker 2006) in higher education to ISP enforcement exercised in most banks will shed light on the feasibility and effectiveness of IT governance in multiple organizational settings. In other words, this study wants to assess how well IT governance aligns with organizational practices encompassing employee's participation empowered by power sharing (Leana 1987) and ISP enforcement supported by coercive force. Subsequently, these findings will enable us to provide suggestions for improving the application of ITG. That is, the *research implication* of this study will propose how to align organizational practices with IT governance for the purpose of fostering information security in different organizational settings.

Literature Review

Banking Industry

The banking culture is mostly hierarchical, bureaucratic, controlled, integrated, and slow to change (Claessens 2012). Overall, the banking industry is a highly regulated industry in that relational systems incorporating a governance unit that oversees banking operation (Scott 2008, pg. 186). The governance unit, administered by authorities and legitimate parties, manages banking regulative and normative controls (Scott 2008, pg. 186). For example, in the United States, Federal Deposit Insurance Corporation (FDIC) and Office of the Comptroller of the Currency (OCC) are related the U.S banks; and this gradually builds a relational system that defines the regulatory environment (Park and Weber 2006). As a result, this propels banks to outline formal policies and procedures in organizational settings.

Following the financial scandal involving Enron and WorldCom, the banking industry has been under immense pressure to comply with regulations such as Sarbanes-Oxley Act (SOX) of 2002, which mandates standard accounting and financial reporting. Banks are also required to comply with

Gramm Leach Bliley Act (GLBA), a comprehensive federal law that requires financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of customer information. To stay compliant, banks adopt IT governance frameworks. In particular, most banks adopt COBIT that aligns well SOX compliant (Chan and McCollum 2004). COBIT has also been used for auditing purposes (Panopoulos 2012)

In general, banks realize security threats and risks (Yeh and Chang 2007) because the banking industry is a target for cybercrimes (Verizon 2015). It was reported that, in 2015, a cybercrime group named "Anunak hackers group" or "Carbanak" stole 1 billion dollars from more than 100 banks worldwide through malware attack (Lennon 2015). This suggests that Cyberattack against banks is innovative, thus making information security protection a moving target. As a result, this creates challenges for banks to implement effective security countermeasures that could thwart the innovative, sophisticated attack. Nevertheless, stakeholders (i.e. customers, board of directors, etc.) expect banks to stop data leakage, misrouting of funds and data errors (Earp and Payton 2006).

Higher Education

Empowering social construction, multiculturalism, and heterogeneity (Tierney, 2001), higher education appreciates differences in lieu of assimilation (Tierney, 1997). Academic freedom is the essence of higher education that sharply distinguishes higher education from other industries (Reis 1997). In general, academic freedom endows scholars with the rights of discovering, discussing, and sharing ideas (Reis 1997). Academic freedom may pose a challenge to security practices. This is because some of the security practices may prolong information processing and sharing, thereby violating academic freedom.

With academic freedom, faculty members are given the autonomy to design their courses and work on their research. This leads to another distinguished characteristic of higher education, that is, professional autonomy (Dill 1999). Professional autonomy empowers faculty members, enabling them to resist security practices. Another challenge of implementing security is the culture of decentralization. In higher education, a large dispersed system due to weak interdependency across departments and systems contributes to the culture of decentralization (Weick, 1976). The heterogeneity of system across different departments brings about difficulty for uniform implementation of security practices.

In the United States, universities and colleges are mandated to comply with the Family Educational Rights and Privacy Act (FERPA) of 1974. FERPA laws permits universities and colleges to disclose directory information including name, address, phone number and email address, dates of attendance, degree(s) awarded, enrolment status, and major field of study without student's consent. However, universities and colleges are disallowed to reveal non-directory information consisting of social security number, student identification number, race, ethnicity, and/or nationality, gender, transcript, and grade reports without student's consent.

Higher education in the United States must also abide by Gramm Leach Bliley Act (GLBA) because the institution is managing student financial aids. Therefore, universities and colleges are obliged to protect student's financial data. Some universities run medical programs so they must comply with Health Insurance Portability and Accountability Act (HIPAA) to protect patient's privacy.

To attain regulatory compliance, higher education starts to adopt IT governance (Stiles 2012). About 55% of universities and colleges integrate IT governance framework into higher education settings (Grama 2015). It is anticipated that more universities and colleges in the United States will employ IT governance framework for security protection because higher education is saddled with higher security threats and higher public scrutiny and accountability (Yanosky and McCredie 2008).

Despite IT governance, higher education has suffered from data breaches. In 2014, data breaches occurred in 5 campuses in the United States - University of Maryland, North Dakota University, Butler University, Indiana University, and Arkansas State University - is more devastating than the Sony's hack (McCarthy 2015). Among those campuses, University of Maryland experienced the largest data breaches, exposing 300,000 student, faculty and staff records (McCarthy 2015).

The following table depicts the differences between higher education and banking:

	Banking	Higher Education
Regulatory Compliance	Comply with SOX and GLBA.	Comply with FERPA, GLBA and HIPAA.
IT Governance	Most banks adopt COBIT that aligns well SOX compliant (Chan and McCollum 2004); COBIT has also been used for auditing purposes (Panopoulos 2012).	About 55% of universities and colleges in the United States integrate IT governance framework into higher education settings (Grama 2015).
Governance Structure	There is a governance unit consisting of external constituents that have authority to oversee the banking operations.	Shared governance is practiced in the institution of higher education (Yanosky and McCredie 2008)
Stakeholder's Expectation	Stakeholders expect banks to stop data leakage, misrouting of funds and data errors (Earp and Payton 2006).	Stakeholders expect higher education to produce innovative research along with creating and sharing knowledge (Reis 1997).
Data Breaches	In 2015, a cybercrime group named "Anunak" stole 1 billion dollars from more than 100 banks worldwide through malware attack (Lennon 2015).	In 2014, data breaches occurred in U. of Maryland, North Dakota U., Butler U., Indiana U., and Arkansas State U. are larger than the Sony's hack (McCarthy 2015).
Challenges for Implementing Security Controls	Information security protection is a moving target because Cyber criminals always come out with better, innovative methods to steal valuable information and money.	Decentralization and academic freedom coupled with professor's professional autonomy may delay the implementation of security practices.

Table 1. Higher Education vs. Banking

Hypotheses Development

This study adopts the model of Industry-Driven Culture Formation suggesting that industry environment compels organizations within the same industry to adopt certain management and organizational practices to produce favorable outcomes in support of organizational survival (Gordon 1991). In particular, the Model of Industry-Driven Culture Formation proposes that management controls organizational structures, processes, and strategies (Gordon 1991). Mainly, organizational structures, processes, and strategies pertain to organizational practices (Kostova and Roth 2002) hinged on the underlying values and beliefs, the written and unwritten rules, and the influence of organization's history, people and interest (Kostova 1999). In short, management drives organizational practices that generates favorable outcomes for organizational survival (Gordon 1991).

Along the same line, this study posits that the management style of organizations drives organizational security practices, which, in turn, generate outcome constituting organizational security norms for information security protection. By examining how banks and higher education arrive at the outcome, that is, organizational security norms, this study could then suggest the implementation of IT governance consistent with management and organizational practices for helping organizations to stay compliant and attain information assurance.

The following subsection presents management style (open vs. rigid) and organizational practices (employee participation vs. ISP enforcement) from the far end of each spectrum. As noted earlier, this study wants to examine the differences in management and organizational practices between higher education and banking industry. We argue that both industries present extreme differences in management and organizational practices, and therefore, we present management and organizational practices from each spectrum to understand the differences in governance between both industries.

Management and Organizational Practices

Management can manifest in either open and flexible or rigid and controlling (Dastmalchian, Lee and Ng 2000). In the same token, Hofstede et al. (1990) suggest that management can facilitate either tight (rigid) or loose (flexible) control. Open and flexible management allows rooms for innovation, quick decision making, and collaboration but rigid management mandates strict monitoring of employee's activities and highlights policies and procedures (Dastmalchian et al. 2000).

Management controls the systems, structures, processes, and strategies (Gordon 1991) that define organizational practices (Kostova and Roth 2002); and therefore, management shapes organizational practices. A change in management instigates changes in organizational practices (Mezias 1990). Organizational practice is *"an organization's routine use of knowledge for conducting a particular function that has evolved over time under the influence of the organization's history, people, interests, and actions"* (Kostova and Roth 2002, pg. 216). Organizational practices across organizations emphasize different focus and content (Kostova 1999). The degree of formalization for organizational practices range from highly formalized (i.e., written rules and procedures) to completely informal (Kostova 1999). Less formalized organizational practices subsumes higher social content; and this may encourage employee's participation by soliciting employee's input (Kostova 1999) when drafting ISP. However, more formalized practices may actively emphasize ISP enforcement. Accordingly, this study outlines organizational practices that (1) encourage employee participation in decision-making related to information security (i.e. policy review); and (2) enforce information security policies (ISP).

Because open management facilitates collaboration (Dastmalchian et al. 2000), this study proposes that open management encourages employee's participation in decision making rather than fostering coordinated controls required in ISP enforcement. Essentially, employee's participation involves power sharing and collaboration (Leana 1987). Therefore, this study argues that, rather than facilitating ISP enforcement, open management encourages employees to participate in decision making related to ISP compliance through collaboration.

H1a: Open management supports employee's participation in decision making related to ISP in higher education and in banking industry

H1b: Open management does not support ISP enforcement in higher education and in banking industry

Since rigid management carries out rule enforcement that discourages employee's participation in decision making related to organizational policies (Aiken and Hage 1966), this study suggests that rigid management supports ISP enforcement but does not facilitate employee's participation in decision making related to ISP compliance.

H2a: Rigid management does not support employee's participation in decision making related to ISP in higher education and in banking industry

H2b: Rigid management supports ISP enforcement in higher education and in banking industry

Organizational Security Norms

As discussed earlier, organizational practices shape the outcomes to assure organizational survival (Gordon 1991). Confronting cyber threats, part of the organizational survival relies on good security practices. Therefore, organizational practices must produce favorable outcome to help organizations survive amidst ubiquitous Cyberattack.

In this study, the outcome constitutes organizational security norms. Organizational norms generate powerful and consistent effects on member's behavior (Hackman 1976) using informal rules (Feldman 1984). That is, organizational norms outlines the right thing to do in organizations. If employees perceive that the right thing to do is to comply with ISP, then they will be more likely to comply (Herath and Rao 2009). In this respect, organizational security norms reflect upon the normative beliefs in organizational security. Organizational security norms shape employee's compliance behavior to secure IT infrastructure (Dhillon 2001) so that organizations can survive the threats of Cyberattack.

This study proposes that organizational security norms are driven by organizational practices encompassing (1) employee's participation in decision making and (2) ISP enforcement. Drawing on the Buy-in Theory, users are more willing to accept a system that was developed with their inputs because user's psychological involvement in information system development (ISD) makes them think that the system is personally important (Markus and Mao 2004). Spears and Barki (2010) built on the same theory to posit that employee's participation in information security measures (e.g. risk management) fosters employee's intention to safeguard information security. In the same token, we propose that encouraging employee's participation in decision making related to ISP will make employees feel that ISP is personally important. This will then increase the employee's perception of information security, leading to a higher degree of organizational security norms.

H3: Employee's participation in decision making for ISP promotes organizational security norms

Additionally, enforcing ISP require organizations to emphasize the importance of security policies. Eventually, the efforts of indicating security policies enhance the perceived mandatoriness of ISP among the employees (Boss et al. 2009) and subsequently shape organizational security norms.

H4: ISP enforcement promotes organizational security norms

The following diagram presents the proposed research model

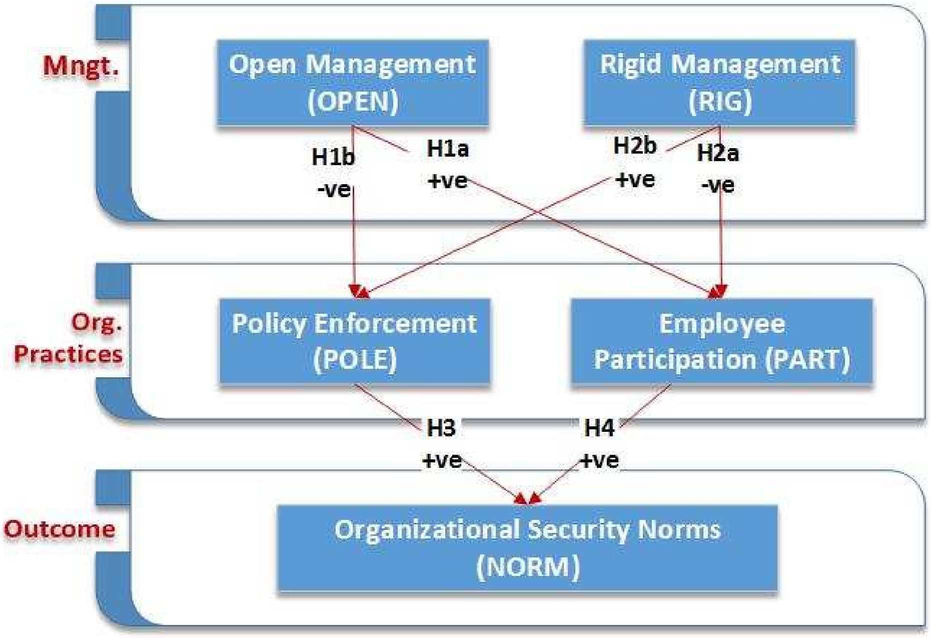

Figure 1. Proposed Research Model

Research Methodology

First of all, we adopted questionnaires from the previous studies (Dastmalchian at al. 2000; Spears and Barki 2010; Herath and Rao 2009) and developed some questions. There are a total of 5 reflective constructs – open management (OPEN), rigid management (RIG), ISP Enforcement (POLE), employee's participation (PART) and organizational security norms (NORM). See figure 1.

Next, this study applied Partial Least Square (PLS) using SmartPLS 3.0 software. At this point, this study has collected data from the college administrators and faculty (N=95) and banking managers (N=85) in the Midwest of the United States. The average age for Higher Education sample is 32 for banking industry is 37. This study will continue to collect more data in the near future.

Overall, this study proves construct validity and reliability in both samples. The following table shows that the average variance extracted (AVE) for each construct in each sample exceeds 0.5, thereby proving convergence validity (Fornell and Larcker 1981). Additionally, the Cronbach's Alpha and Composite Reliability for each construct in each sample is larger than 0.7, thus demonstrating construct reliability (Fornell and Larcker 1981; Chin 1998).

The following table depicts the AVE, Cronbach's Alpha, and Composite Reliability of each construct:

Construct	Banking (N=85)			Higher Education (N=95)		
	AVE	Cronbach's Alpha	Composite Reliability	AVE	Cronbach's Alpha	Composite Reliability
NORM	0.832	0.899	0.937	0.784	0.861	0.916
OPEN	0.788	0.869	0.918	0.728	0.816	0.889
PART	0.714	0.812	0.882	0.710	0.791	0.879
POLE	0.857	0.916	0.947	0.825	0.894	0.934
RIG	0.747	0.832	0.899	0.662	0.743	0.853

Table 2. Construct Reliability and Validity

To test the hypotheses and compare the significant differences in the proposed relationships (see Figure 1) between both samples, this study ran Multi-Group Analysis (PLS-MGA). Using parametric test, this study examines the significant differences in the relationships between higher education and banking industry. The preliminary study presents the following results for hypotheses testing:

The following table depicts the differences between higher education and banking:

Hypotheses	β (t-value)		Difference in Coefficients (t-value)
	Banking	Higher Education	
H1a: OPEN → PART	0.071 (0.993)	0.359 (6.532)***	0.288 (3.265)**
H1b: OPEN → POLE	-0.083 (1.561)	0.147 (1.750)	0.230 (2.158)*
H2a: RIG → PART	0.590 (8.012)***	0.393 (4.563)***	0.197 (1.679)
H2b: RIG → POLE	0.653 (10.819)***	0.137 (1.730)	0.516 (4.947)***
H3: POLE → NORM	0.477 (6.601)***	0.420 (5.613)***	0.057 (0.539)
H4: PART → NORM	0.270 (3.393)***	0.241 (2.767)**	0.029 (0.239)

Table 3. Results of Hypotheses Testing (*p < 0.05, ** p < 0.01, ***p < 0.001)

Next, the table below presents the R-Square values for both samples:

Construct	R-Square (t-value)	
	Banking	Higher Education
NORM	0.437 (5.549)***	0.289 (4.485)***
PART	0.390 (5.492)***	0.379 (4.467)***
POLE	0.384 (4.943)***	0.054 (1.287)

Table 4. R-Square Values (*p < 0.001)**

Analysis Results and Discussion

H1: Open management fosters employee's participation (β=0.359, p < 0.001) but does not encourage ISP enforcement (β=0.147, p > 0.05) in higher education. However, open management drives neither employee's participation (β=0.071, p > 0.05) nor ISP enforcement (β=-0.083, p > 0.05) in the banking industry. Therefore, H1a is partially supported and H1b is fully supported.

Additionally, the results reveal that, between banking industry and higher education, there is a significant difference in the relationship between open management on employee's participation in decision making (β difference=0.288, p < 0.01) wherein open management in higher education is more effective in driving employee's participation than that in the banking industry.

H2: Interestingly, rigid management motivates employee's participation (β=0.590, p < 0.001) and ISP enforcement (β=0.653, p < 0.001) in the banking industry. Analysis results also reveal that rigid management facilitates employee's participation (β=0.393, p < 0.001) but does not encourage ISP enforcement (β=0.137, p > 0.05). Thus, H2a is not supported and H2b is partially supported.

A significant difference exists in the relationship between rigid management and ISP enforcement between both industries (β difference = 0.516, $p < 0.001$). It is also worth noting that the R^2 value for ISP enforcement (POLE) is insignificant ($R^2 = 0.054$, $p > 0.05$) for higher education but significant for banking industry ($R^2=0.384$, $p < 0.001$) (See Table 4). This suggests that rigid management is more effective in enforcing ISP in banking industry than that in higher education.

H3 and H4: Employee's participation in decision-making (β=0.270, $p < 0.001$) and ISP enforcement (β=0.477, $p < 0.001$) build organizational security norms in the banking industry. Similarly, employee's participation (β=0.241, $p < 0.01$) and ISP enforcement (β=0.420, $p < 0.001$) shape organizational security norms in higher education. Therefore, H3 and H4 are supported.

Conclusion, Future Research and Contribution

In conclusion, this study reveals two key findings. First, in comparison to the banking industry, open management in higher education is more effective in facilitating employee's participation in decision-making for ISP compliance. This infers that shared governance must be addressed to attain ISP compliance in higher education. Although analysis results reveal that rigid management also fosters employee's participation in higher education, we argue that rigid management focusing on strict monitoring is not applicable in the higher education setting. This is mainly because higher education espouses social construction, multiculturalism, and heterogeneity (Tierney, 2001) that cannot be attained with strict monitoring.

Second, our finding reveals that rigid management encourages employee's participation in decision making in the banking industry. This suggests that, despite hierarchical structure, banks facilitates employee's participation. This thereby supports the notion that IT governance can operate in a decentralized mode that involves certain degree of power sharing with management (Sambamurthy and Zmud 1999).

Accordingly, we contend that the future research will contribute to IT governance in two different ways. First, the preliminary findings suggest that open management is more applicable to the institution of higher education for fostering organizational security norms. In the future, we will further examine how to align IT governance with open management in higher education. To the best of our knowledge, there are not many studies investigating this aspect, and therefore, the future research findings will be the one of the key contributions to IT governance research.

Specifically, our findings demonstrate that, in higher education, ISP enforcement is not facilitated by rigid management. This infers that top management in support of ISP enforcement will not produce fruitful results for information security safeguards in higher education. That is, unlike most industries, coercive force associated with ISP enforcement does not blend well with higher education culture. In the near future, the research implication will suggest a different paradigm of IT governance framework customized to higher education.

Second, our findings exhibit that rigid management encourages employee's participation in the banking industry. This is a "fresh" perspective that can be further explored to derive meaningful findings. Presently, most of IT governance frameworks supporting top-down/rigid management do not address involving employees to participate in the decision-making related to information security. Therefore, the future research will share how to integrate employee participation into IT governance for the traditional corporate setting. In specific, Sambamurthy and Zmud (1999) posited that IT governance may occur in a decentralized mode where IT division and management *"assume authority for all IT activities"* (pg. 262). Focusing on the decentralized mode, the future research will suggest how to improve the collaboration and participation among management and IT employees in IT governance.

Finally, this study presents the preliminary results that show promises in the contributions to the research findings concerning IT governance. We will continue to collect data from the banking industry and higher education and address the aforementioned key points to strengthen our findings.

References

Aiken, M. and Hage, J. (1966). "Organizational Alienation: A Comparative Analysis," *American Sociological Review* 31(4), pp.497-507.

Barve, J. (n.d.). COBIT Case Study: IT Risk Management in a Bank. From http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-IT-Risk-Management-in-a-Bank.aspx

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., and Boss, R.W. (2009). "If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* 18(2), 151-164.

Campbell, J., McDonald, C. and Sethibe, T. (2010). "Public and Private Sector IT Governance: Identifying Contextual Differences," *Australasian Journal of Information Systems* 16(2), 5-18.

Chan, S. and McCollum T. (2004). "Sarbanes-Oxley: The IT Dimension." *The Internal Auditor* 16(1), 31–33

Chin, W.W. (1998). *The Partial Least Squares Approach to Structural Equation Modelling*. New Jersey: Lawrence Erlbaum Associates.

Claessens, R. (2012). *Corporate Culture in Banking*. UK: AuthorHouse.

Dastmalchian, A., Lee, S. and Ng, I. (2000). "The Interplay between Organizational and National Cultures: A Comparison of Organizational Practices in Canada and South Korea using the Competing Values Framework," *The International Journal of Human Resource Management* 11(2), 388-412.

Dill, D. D. (1999). "Academic Accountability and University Adaptation: The Architecture of an Academic Learning Organization," *Higher Education* 38(2), 127–154.

Dhillon, G. (2001). "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns," *Computers & Security* 20(2), 165-172.

Earp, B.E. and Payton, F.C. (2006). "Information Privacy in the Service Sector: An Exploratory Study of Health Care and Banking Professional," *Journal of Organizational Computing and Electronic Commerce* 16(2), 105-122.

Feldman, C. (1984). "The Development and Enforcement of Group Norms," *Academy of Management Review* 9(1), 47-53.

Fornell, C. and Larcker, D. (1981), "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* 18(1), 39-50.

Gilmour, J. E. (1991). "Participative Governance Bodies in Higher Education: Report of a National Study," *New Directions for Higher Education*, 1991(75), 27–39.

Gordon, G.G. 1991. "Industry Determinants of Organizational Culture," *Academy of Management Review* 16(2), 396-415.

Grama, J. L. 2015. *Understanding IT GRC in Higher Education: IT Governance*. From http://er.educause.edu/articles/2015/2/understanding-it-grc-in-higher-education-it-governance

Hackman, J. R. (1976). *Group Influences on Individuals*, In Handbook of Industrial and Organizational Psychology, ed. M. D. Dunnette. Chicago: Rand MacNally.

Hardy, G. (2006). "Using IT governance and COBIT to Deliver Value with IT and Respond to Legal, Regulatory and Compliance Challenges," *Information Security Technical Report* 11(1), 55–61.

Herath T and Rao H. (2009), "Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* 18, 106-125.

Hofstede, G., Neuijen, B., Ohayv, D.D. and Sanders, G. (1990). "Measuring Organizational Cultures: A Qualitative and Quantitative Study across Twenty Cases," *Administrative Science Quarterly* 35(2), 286–316

Hu Q, Dinev T, Hart P and Cooke D (2012). "Managing Employee Compliance with Information Security Policies: The Role of Top Management and Organizational Culture," *Decision Sciences* 43(4), 615-660.

Kostova, T. (1999). "Transnational Transfer of Strategic Organizational Practices: A Contextual Perspective," *Academy of Management Review* 24(2), 2308-2324.

Kostova, T. and Roth, K. (2002). "Adoption of an Organizational Practice by Subsidiaries of Multinational Corporations: Institutional and Relational Effects," *Academy of Management Journal* 45(1), 215-233.

Leana, C.R. (1987). "Power Relinquishment versus Power Sharing: Theoretical Clarification and Empirical Comparison of Delegation and Participation," *Journal of Applied Psychology* 72(2), 228-233

Lennon, M. (2015). *Hackers Hit 100 Banks in "Unprecedented" $1 Billion Cyber Heist: Kaspersky Lab*. SecurityWeek.com. Retrieved from http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab

Markus, M.L. and Mao, Y. (2004). "Participation in Development and Implementation – Updating an Old, tired Concept for Today's IS Contexts," *Journal of the Association for Information Systems*

5, 514–544

McCarthy, K. (2015). *5 Colleges with Data Breaches Larger than Sony's in 2014*. From http://www.huffingtonpost.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html

McCredie, J. (2006). "Improving IT Governance in Higher Education," *EDUCAUSE Center for Applied Research*, 2006(18), 1–12.

Mezias, S.J. (1990). "An Institutional model of Organizational Practice: Financial Reporting at the Fortune 200," *Administrative Science Quarterly* 35(3), 431-457.

Panopoulos, J. (2012). *COBIT Case Study: Integrating COBIT 4.1 into the Internal Audit Function*. From http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Integrating-COBIT-4-1-Into-the-Internal-Audit-Function.aspx

Park, K. and Weber, W. (2006). "A Note on Efficiency and Productivity Growth in the Korean Banking Industry, 1992-2002." *Journal of Banking and Finance* 30(8), 2371-2386

Reis, R.M. (1997). *Tomorrow's Professor: Preparing for Academic Careers in Science and Engineering*, New Jersey: Wiley-IEEE Press.

Sambamurthy, V. and Zmud, R. W. (1999). "Arrangements for Information Technology Governance: A Theory of Multiple Contingencies," *MIS Quarterly* 23(2), 261–290.

Scott, W.R. 2008. *Institutions and Organizations, Ideas and Interest* 3rd Edition, Thousand Oaks: Sage

Spears, J.L. and Barki, H. (2010). "User Participation in Information Systems Security Risk Management," *MIS Quarterly* 34(3), 503-522.

Stiles, R. J. 2012. "Understanding and Managing the Risks of Analytics in Higher Education: A Guide," *EDUCAUSE*. Retrieved from https://net.educause.edu/ir/library/pdf/EPUB1201.pdf

Tierney, W. G. (1997). "Organizational socialization in Higher Education," *Journal of Higher Education* 68(1), 1-16.

Tierney, W. G. (2001). "The Autonomy of Knowledge and the Decline of the Subject: Postmodernism and the Reformulation of the University," *Higher Education* 41(4), 353-372.

Verizon (2015). *2015 Data Breach Investigations Report*. Retrieved from http://www.verizonenterprise.com/DBIR/2015/

Weick, K. (1976). "Educational Organizations as Loosely Coupled Systems," *Administrative Science Quarterly* 21(1), 1–19.

Yanosky, R., and McCredie, J. (2008). "Process and Politics: IT Governance in Higher Education," *EDUCAUSE Center for Applied Research* 2008(5), 1-141.

Yeh, Q. and Chang, A. J. (2007). "Threats and Countermeasures for Information System Security: A Cross-Industry Study," *Information and Management* 44(5), 480-491.

Yukl, G. A. and Becker, W. S. (2006). "Effective Empowerment in Organizations," *Organization Management Journal*, 3(3), 210–231.