Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2009 Proceedings

European Conference on Information Systems (ECIS)

2009

A study of compliance management in information systems research

Norris Syed Abdullah
The University of Queensland, norris@itee.uq.edu.au

Marta Indulska
The University of Queensland, m.indulska@business.uq.edu.au

Sadiq Shazia
University of Queensland, shazia@itee.uq.edu.au

A STUDY OF COMPLIANCE MANAGEMENT IN INFORMATION SYSTEMS RESEARCH

Syed Abdullah, Syed Norris Hikmi, The University of Queensland, 4072 Brisbane, Australia, norris@utm.my

Indulska, Marta, The University of Queensland, 4072 Brisbane, Australia, m.indulska@business.uq,edu.au

Sadiq, Shazia, The University of Queensland, 4072 Brisbane, Australia, shazia@itee.uq,edu.au

Abstract

Regulatory compliance has become a critical concern for many industries around the globe and investment to achieve compliance has increased drastically inline with that concern. While Information Systems (IS) are considered a part of the support architecture, anecdotal evidence suggests that organisations struggle with finding the right tools and guidance on approaches for compliance management. For this reason, we undertake a review of the current research on compliance management topics in the Information Systems domain, with the ultimate goal to carry out a gap-analysis between research-based solutions and the current needs of compliance management professionals. In this paper, we consider thirteen Information Systems journals and perform an exhaustive analysis of the type of compliance management research published at these venues in the last five years. The analysis found forty-five relevant articles, which were then further classified depending on the type of their contribution. The results of the analysis suggest that IS research in managing compliance has received increasing attention in the recent years. The study also suggests that research has predominantly focussed on exploratory studies, rather than proposition of solutions that can assist organizations in their compliance management regimens.

Keywords: IS Journals, Regulation / Deregulation, Literature Review, Business Process Management

1 INTRODUCTION

Today, regulatory compliance has attracted much investment by organisations across the globe (Braganza & Franken 2007). The boost in compliance related investment is primarily a consequence of regulatory mandates that emerged as a result of events that led to some of the largest scandals in corporate history, such as Enron, WorldCom (USA), HIH (Australia) and Societe Generale (France). Compliance essentially means ensuring that business processes, operations and practice are in accordance with a prescribed and/or agreed set of norms. Introduction of regulations such as Sarbanes-Oxley Act of 2002 (SOX), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act of 1999 (GLB) has made regulatory compliance a focal point of many organisations. Organisational units or department such as finance, administrative and information systems are affected by these changes. The investment is necessary for organisations to remain in business (Perskow 2003, Anon et al. 2007), since non-compliance to some government and legal requirements can have dire consequences.

Each new introduced regulation carries with it a potentially significant cost of implementation for those organizations that fall under its control. SOX spending has reached US$6B in 2007 in USA alone, which represents only a fraction of the total compliance effort (Reilly 2007). Meanwhile, analysts predict that overall USA spending on governance, risk and compliance (GRC) will exceed US$32B in 2008 (McGreevy 2008). Hence, increasing compliance expectations are a significant financial drain on organizations and are often considered as a burden rather than a business opportunity. The burden is magnified by the apparent lack of guidance from the research community on the best ways to approach compliance management. In this study, we define compliance management as mechanisms to keep enterprise's businesses safe from possible violation of regulatory compliance. In his work, Kharbili (2008) stated that compliance management also refers to standards, frameworks, and software used to ensure the company's observance of legal texts.

There is ongoing discussion on the roles of Information Systems (IS) as enabling technology that facilitates achieving and demonstrating compliance. Although some of the discussion focuses more on the use of IT as a supporting technology to achieve compliance, research also exists on management related issues, for example, how compliance affects CIO responsibilities in the organisation (Berghel 2005) and (Braganza & Franken 2007). While compliance management does not appear to have become a main stream of IS research at this point in time, the apparent lack of guidance for compliance management professionals motivates us to develop a comprehensive understanding of the focus, extent and shortcomings of compliance management research in the Information Systems community. The final goal is the derivation of an industry-relevant research agenda for compliance management. In order to develop such an agenda, two aspects are required, *viz.* an understanding of the current state of research, and an understanding of current problems exhibited in practice. In this paper we address the first aspect.

We proceed as follows. The next section presents a discussion of the methodology employed to assure a rigorous and relevant analysis of compliance management research. Section 3 presents an in-depth analysis of the relevant research. In section 4 we present a discussion of the results and conclude the paper in Section 5 with a discussion of limitations and future work in this area.

2 RESEARCH APPROACH

We took as our data set the collection of papers published at premium Information Systems journals (as promoted by the Association for Information Systems) and also included some additional popular journals in the discipline. Namely, the list of considered journals includes: Business Process Management Journal (BPMJ), Communication of the Association for Information Systems (CAIS),

Communication of the Association for Computing Machinery (CACM), European Journal of Information Systems (EJIS), Journal of Information and Management (JI&M), Journal of Information Systems Research (JISR), Journal of the Association for Information Systems (JAIS), MIS Quarterly (MISQ), Journal of Information Systems – Sarasota (JIS), Information Systems Frontier (ISF), Information Systems Journal-Blackwell (ISJ), Information Systems – Elsevier (IS), and Journal of Management Information Systems (JMIS).

We expected that the majority of the research would be published since 2006, however we considered all papers published at these outlets in 2001-2008 so as to identify any changes in trends and also a change in foci of compliance management research (e.g. a shift of focus to SOX). In total, the data set consisted of 5633 articles. Each paper was prepared and included in a full text search for the purposes of identifying contributions relevant to the compliance management domain. Full text searches were conducted on the data set, using a keyword of "compliance" and "compliant". Following a stage of eliminating paper duplicates in the search results (i.e. ensuring that a paper that matched both search criteria is only counted once). This analysis provided us with a set of 510 articles. As a further step to assess paper relevance to the domain of compliance management, we inspected the occurrence of the search terms in the paper text, and included only those that had three or more hits. This step reduced and focused the data set on 178 papers.

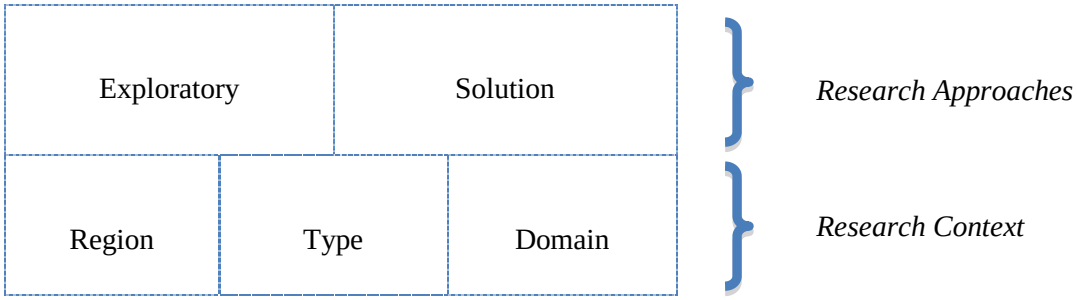

Figure 1. Analysis Framework

With the reduced set of papers, a review of each paper and its contribution was carried out. This review included reading the abstract, introduction, and scanning through the main contributions of the remainder of the paper as well as its conclusions. This stage was the most critical part of the study, since it provided an understanding of the contribution of the paper and what aspects of regulatory compliance were addressed (and in what way). This stage of the analysis was helped through a framework that was developed to analyse the contributions of compliance management research. The framework is presented in Figure 1. Within this framework, we differentiate between case study and exploratory papers, versus papers that provide a solution to a compliance management related problem. These identify the two main classes of ***research approaches***. The solution papers were further classified in terms of their focus on preventative, detective or corrective measures. The papers were also classified by geographic region of application of the paper (North America, South America, Africa, Asia-Pacific, Europe), domain of application or industry sector (Financial, Healthcare, E-Commerce, etc) and type of compliance considered (to (1) Regulations or Legislation, (2) Standards and Code of Practice, (3) Business Contracts, Service Agreements etc. and (4) Corporate Policy). The latter classification is intended to provide ***research context***.

This last stage of the analysis and the careful reading of each paper resulted in a further reduction of the data set. Despite the papers having more than three references to "compliance" or being "compliant", many were determined not to present a main contribution to the domain of compliance management. Instead, they mentioned compliance in various parts of the discussion and future work, however did not focus on the topic, or the notion of compliance was significantly different, e.g.

compliance to a network protocol, or XML format, etc. Accordingly, the analysis reduced the set of papers from 178 to 45.

3 ANALYSIS

Table 1 shows the breakdown of papers relevant to compliance management and their source of publication. Out of 5633 articles, only 45 articles match the regulatory compliance context as explained above. This represents 1.3% of BPMJ articles, 2.4% of CAIS articles, 0.8% each for CACM and JI&M, 0.6% EJIS, 0.7% of JISR, 1.4% of JAIS, and 0.4% for MISQ. Five other journals (JIS, ISF, ISJ, IS and JMIS) did not contain any articles that match the compliance context. We expect that the significantly higher number of matches in the CAIS and CACM journals, may be influenced by the nature of the journal itself, which caters to exploratory type articles. At the early stage of the compliance management research in Information Systems, one would expect that there would be an increased focus on exploratory papers first, so as to understand the problems at hand, before a surge in papers presenting Information Systems solutions. Although the relatively low number of publications may be seen as not encouraging, the IS research community should not take it as an indicator of insignificance. Indeed, the roles of IS or IT as enablers of regulatory compliance have increased year by year (Smith & McKeen 2006).

	TOTAL	Matched with Regulatory Compliance	Percentage (%)
JOURNALS			
CAIS	594	14	2.4
JAIS	147	2	1.4
BPMJ	320	4	1.3
JI&M	491	4	0.8
CACM	2100	17	0.8
JISR	150	1	0.7
EJIS	350	2	0.6
MISQ	271	1	0.4
JIS-Sarasota	117	-	-
ISF	195	-	-
ISJ-Blackwell	185	-	-
ISJ-Elsevier	385	-	-
JMIS	328	-	-
TOTAL	**5633**	**45**	**0.8**

Table 1. Sources and Frequency of Publication

The next step in the analysis carried out the classification with respect to the type of publication, *viz.* case study/exploratory and solution. As expected in an emerging research domain, the majority of the publications were found to be in the case study or exploratory paper category - 35 (76.1%) of the articles are case study/exploratory articles and nine (19.6%) are solution articles. However, there are two (4.3%) articles that matched both types of articles. The results suggest that research on regulatory

compliance solution has being initiated but remains still in the early exploratory stages, not yet progressing to a stage where many Information Systems solutions are proposed or discussed. This finding is inline with the need to identify the problems at hand first, before proposing solutions. Figure 2 presents the breakdown of the papers by type of contribution.

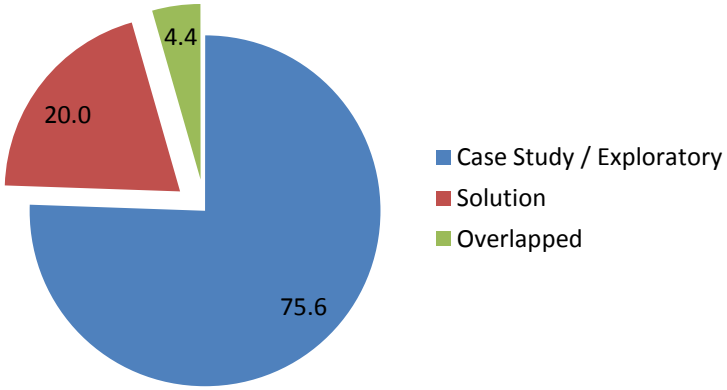

Figure 2. Distribution of Articles by Type

Furthermore, we were interested to determine the emergence of compliance management research in Information Systems publication outlets. The breakdown of compliance management per year of publication is shown in Figure 3. The figure clearly shows that a spike in publications was recorded in 2006. We posit that this finding is in line with the increased focus on SOX Act of 2002 and also an early focus on HIPAA. A characteristic of publishing in the Information Systems discipline is a lag of generally one to two years from time of writing to time of actual publication. Accordingly, this situation would imply that increasing focus began around 2002, when HIPAA was being seriously considered and the SOX Act was introduced. Prior to this event, little literature on compliance management exists, despite some other regulations having already been proposed (e.g. HIPAA). We expect the increasing trend to continue in 2008, despite the perceived drop in compliance management publications. One of the limitations of the study pertaining to the specific year of 2008 is that while some of the newly published contributions have already been indexed, many have not. Due to this restriction, Figure 3 only includes some of the early 2008 research.

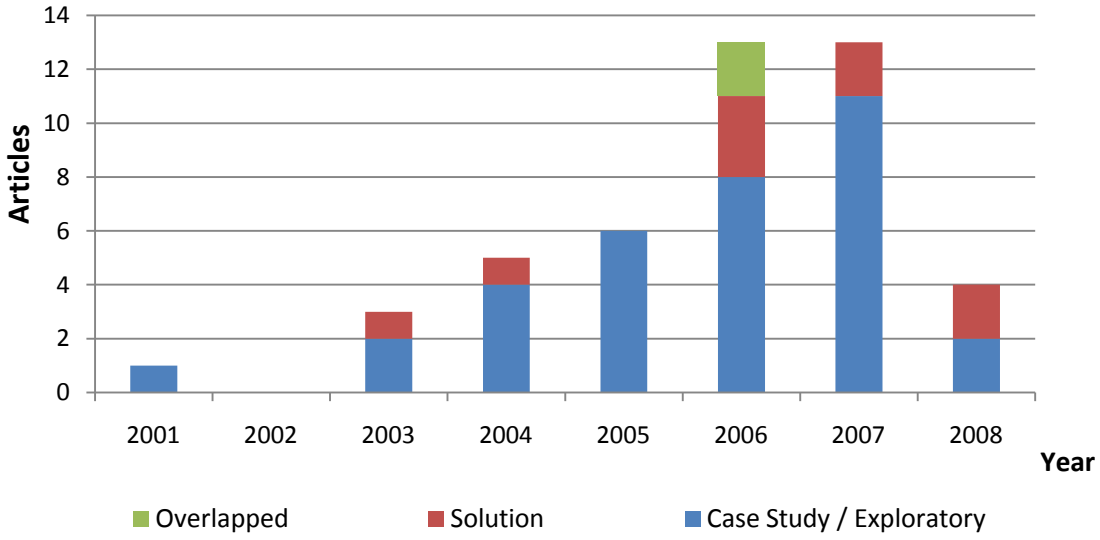

Figure 3. Distribution of Article per Type per Year

Further analysis was done to identify the type of domain application that was the focus of the paper. Figure 4 shows the results of that analysis, which found that the application of regulatory compliance discussed in the articles was dominated by three domains, *viz.* auditing, finance and healthcare, which made up 76% of the articles. On the other hand, domains such as e-commerce and the environment were only discussed in 13% of the articles proportion. The remaining articles, which represent 11% of the focused data set, did not have a specific domain of application with regard to regulatory compliance.

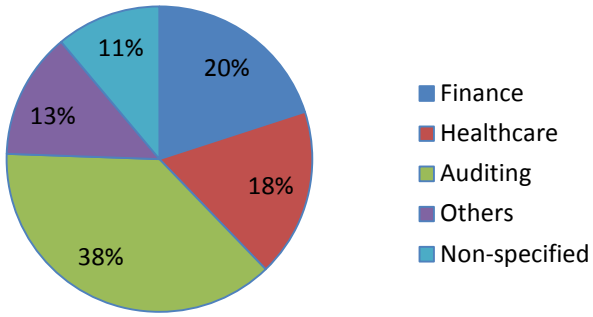

Figure 4. Articles by Domain of Applications

In looking at the distribution of articles per region, we have been able to identify the main geographical areas of application as reported in the papers. The analysis was performed by inspecting not the country of publishing authors but rather the locality of case studies or exploration on regulatory compliance discussed in the articles. The analysis found that 22 out of 37 case study/exploratory articles represent the North America region. This proportion of almost 60% of the articles that focus on the North America region might be due to most of the regulatory compliance requirements being introduced earlier in the North America region than others. The finding indicates that there is a need to explore compliance management in different regions, in particular focusing on whether differences exist between practices in the various regions. The focus on other regions is not, however, non-existent, with two and three articles representing Asia-Pacific and Europe regions respectively. The other 10 articles were categorised as non-specified because they applied to either all regions or did not explicitly state the region of the case study.

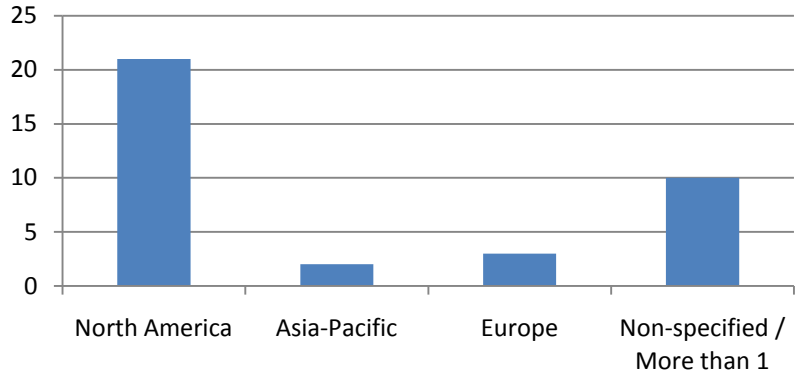

Figure 5. Articles Population by Region

The careful classification of the papers also resulted in the elucidation of details in terms of the regulations that are the focus of the Information Systems research community. The analysis found that 42 out of 46 articles had specified the regulations that the research was relevant to. While eight articles discussed the details on regulatory compliance type only in general without focusing to specific

regulation name (e.g. contract compliance in general), the 34 remaining articles specifically named a single regulation in the discussion. Detail for the distribution of articles by their regulatory focus is presented in Table 2.

Regulation/Policy/Standard/Contract	No. of Articles
General	8
HIPAA	8
SOX	6
ISO	6
SLA	2
CFIP	2
Others	9

Table 2. Distribution of Regulatory Compliance Type by Name

Most prominently, HIPAA (Health Insurance Portability and Accountability Act of 1996) had the highest perceived focus, being the focus of eight publications. SOX (Sarbanes-Oxley Act of 2002) and ISO (ISO17799, ISO14000, ISO9000, and ISO9001:2000) followed with six articles each. Lesser focus was placed on SLA (Service Level Agreement) and CFIP (Code of Fair Information Practice). Nine papers mentioned a variety of regulations. These include Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), New Zealand Privacy Act, Electronic Record Management Policy, European 1995 Personal Data Protection Directive, Accreditation Board for Engineering and Technology / Computing Accreditation Commission Standard (ABET/CAC), American Election Committee Voting System Standards (AEC), Eco-Management Audit Scheme (EMAS), Capability Maturity Model Integration - Software Engineering(CMMI-SW), and Fair Credit Reporting Act 1970.

We were further motivated to investigate whether clear specific foci exist with the main geographic regions of interest. In the North America region, the focus is led by Auditing applications (with seven articles). This focus was followed by Healthcare and Finance applications with six and seven articles respectively. While Auditing remains as focus of the application in Asia-Pacific and Europe with one article for each region, Healthcare applications did not attract any discussion from Asia-Pacific and Europe regions.

Furthermore, we reviewed the same articles by discovering the type of regulatory compliance being discussed in those articles with consideration of the region of application. The review shows that most of North America region articles (17 articles) focus on regulatory compliance. This focus is followed by a focus on compliance with standards as second popular type in North America (with 3 articles). The foci for Asia-Pacific region include regulatory compliance and contract compliance, with one article for each type. The Europe region also appears to focus on standard and regulation compliance, with two and one articles respectively. Our analysis did not identify any contributions that specifically address compliance with policies.

Further to the detailed investigation carried out on the case study/exploratory articles, the articles that were classified as solution providing articles were also reviewed in terms of the type of solution presented. This process involved identification of articles that referred to solution approaches. These articles were classified as either preventive, detective, or corrective in nature. The study reveals that 7 out of 11 articles offer a preventive solution, while the remaining (four) articles offer a detective solution. No corrective solutions we identified in the data set. The situation might be explained be a preference in compliance management for preventive solutions, given the high penalties for non-compliance with some regulations (not only in terms of costs but also in terms of reputational damage,

etc). The actual solutions presented in the papers vary from contribution to contribution. Some of the solutions, for example, (Agrawal et al. 2007) and (Weitzner et al. 2008) addressed the detective type of solution. In particular, (Agrawal et al. 2007) introduced the Hippocratic Database Compliance Auditing component, which facilitates the privacy officer to conduct a series of audits, in a matter of minutes, to reliably isolate potential sources of information leaks in electronic health records. (Banker et al. 2007), have discussed a simple model in which contract monitoring cost in addition to search and coordination cost is introduced to capture the complexity in buyer-supplier relationships. Another work, (Volonino 2003) presented an overview of e-evidence and computer forensics and their implication to IS. Thus there is significant diversity in the various solution papers.

4 DISCUSSION

The findings from the analysis have provided us with a number of interesting facts with regard to the current focus of IS journal articles associated with regulatory compliance. We summarize these as follows:

- Research Trends and Focus
  The trends of regulatory compliance IS research articles show significant growth starting in year 2003. The majority of these contributions feature exploratory research as compared to research that provides specific solutions. Our findings also reveal that the articles are dominated by work that discusses regulatory compliance associated with North America cases. This research is also linked to a number of regulations that have been introduced in the region i.e. HIPAA, GLB, COPPA, SOX, and CAN-SPAM Act.

- Domain of Application
  Auditing, Healthcare and Finance are the domains that attracted most concern in the articles. This implies the critical applications of compliance. However, since these domains are predominant in North America region the necessity of other domain of applications might emerge differently in other region.

- Type of Regulatory Compliance
  Perhaps because articles were dominated by North America region, regulation is the anticipated type of compliance and is shown to have attracted most discussion. In contrast, other types such as policy, contract and even standard did not get as much attention. This further show that most of the solutions discussed also focus on achieving compliance with regulations.

- Focus of the Solutions
  All solution associated with regulatory compliance discussed in the articles focus either on preventive or detective type of solutions. It may be hard in general for IS community to contribute to this aspect as corrective measures are an outcome of business/legal advice and strategy. However, it needs to note that it is not always possible to mitigate the risk even when a compliance product is involved and hence corrective measures become inevitable (Mercuri 2004).

- Regional
  As mentioned earlier, North America cases feature prominently in the discussion of regulatory compliance in IS research. Future work is clearly needed to study the impact of regulatory compliance in other regions.

5 CONCLUSION

This paper presents a first comprehensive snapshot of the development and focus of compliance management related research in the Information Systems discipline. The analysis is motivated by the recent changes that drastically change the IS/IT functions within organisations so as to achieve compliance. The articles were gathered from 13 IS Journals, which consist of articles from 2001 until early 2008. The sources for the analysis, which constitute of 5633 articles, were filtered through three stages of filtration that finally narrow it down to 45 articles. The filtered articles were then subject to classification and analysis based on a proposed framework. The study reveals that the majority of the related IS publications are exploratory in nature. We posit this to be an indication of the relative immaturity of the research in this domain, where problems are still being identified rather than solutions being provided. While we concede that many solutions might perhaps be published in more technical venues (Sadiq et al. 2006), the role of Information Systems in supporting and demonstrating compliance should be exhibited with solutions papers in the IS domain also.

The work has a number of limitations. While all care was taken to download the full set of journal papers that represents the selected journals and years, this selection was limited to soft copy papers only. Papers available in print version (and not already digitised) were excluded from this analysis. Given the focus on recent years, we do not expect this limitation to have a significant impact on the data set. Additional limitations stem from the currently incomplete set of papers for the year 2008. Only a small number of papers published this year have been indexed, these papers will be included in the analysis as soon as they become available so as to present an up to date snapshot of compliance management research.

Future work in this area involves two major steps. The first is an extension of the IS journals to also IS conference venues, which have a shorter time to publication and would provide more detail on the development of maturity in the compliance management research area. Second, a series of interviews and focus groups has been initiated in order to collect the compliance management problems, as experienced by compliance management professionals, and as observed by compliance management consultants and auditors. The ultimate goal is to perform a gap-analysis between industry needs and the focus of the research community, resulting in an industry-relevant research agenda for the coming years.

References

Agrawal, R., Tyrone G., C. Johnson and Kiernan J. (2007). Enabling the 21st Century: Health Care Information Technology Revolution. Communications of the ACM, Vol. 50(No. 2): 35-42.

Anon, J. L., H. Filowitz and Kovatch, J.M. (2007). Integrating Sarbanes-Oxley Controls into an Investment Firm Governance Framework. The Journal of Investment Compliance, Vol. 8(No. 1): 40-43.

Banker, R. D., Kalvenes, J. and Patterson, R. A. (2007). Information Technology, Contract Completeness, and Buyer-Supplier Relationships. Information Systems Research, Vol. 17, 180-193.

Berghel, H. (2005). The Two Sides of ROI: Return on Investment vs. Risk of Incarceration. Communications of the ACM, Vol. 48(No. 4): 15-20.

Braganza, A. and A. Franken (2007). SOX, Compliance and Power Relationships. Communications of the ACM, Vol. 50(No. 9): 97-102.

Kharbili, M.E., Stein, S., Markovic, I. and Pulvermüller, E. (2008). Towards a Framework for Semantic Business Process Compliance Management. in GRCIS 2008. Montpellier, France.

McGreevy, M. (2008). AMR Research Finds Spending on Governance,Risk Management, and Compliance Will Exceed $32B in 2008. AMR Research, Inc.

Mercuri, R. T. (2004). The HIPAA-potamus in Health Care Data Security. Communications of the ACM Vol. 47(No. 7): 25-28.
Perskow, B. I. (2003). Sarbanes Oxley: Investment Company Compliance. The Journal of Investment Compliance, Vol. 3(No. 4): 16 - 30.
Reilly, K. (2007). AMR Research Finds Spending on Sarbanes-Oxley Compliance will Remain Steady at $6.0B in 2007. AMR Research, Inc.
Sadiq, S., Governatori, G. and Naimiri, K. (2007). Modeling of Internal Controls for Business Process Compliance. International Conference on Business Process Management BPM 2007. Brisbane, Australia, Sep 2007.
Smith, H. A. and J. D. McKeen (2006). Developments in Practice XXI: IT in the New World of Corporate Governance Reforms. Communications of the Association for Information Systems Volume 17: 714-727.
Volonino, L. (2003). Electronic Evidence and Computer Forensics. Communications of the Association for Information Systems, Volume 12, 457-468.
Weitzner, D. J., H. Abelson, T. Berners-Lee, Feigenbaum, J., J. Hendler and G. J. Sussman (2008). Information Accountability. Communications of the ACM Vol. 51(No. 6): 82-87.