Emerging Challenges in Information Systems Research for Regulatory Compliance Management

Norris Syed Abdullah[1], Shazia Sadiq[1], and Marta Indulska[2]

[1] School of Information Technology & Electrical Engineering, The University of Queensland, 4072 Brisbane, Australia
{norris,shazia}@itee.uq.edu.au
[2] UQ Business School, The University of Queensland, 4072 Brisbane, Australia
m.indulska@business@uq.edu.au

Abstract. Managing regulatory compliance is increasingly challenging and costly for organizations world-wide. While such efforts are often supported by information technology (IT) and information systems (IS) tools, there is evidence that the current solutions are inadequate and do not fully address the needs of organizations. Often such discrepancy stems from a lack of alignment between the needs of the industry and the focus of academic research efforts. In this paper, we present the results of an empirical study that investigates challenges in managing regulatory compliance, derived from expert professionals in the Australian compliance industry. The results provide insights into problematic areas within the compliance management domain, as related to regulatees, regulations and IT compliance management solutions. By relating the identified challenges to existing activity in IS research, this exploratory paper highlights the inadequacy of current research and presents the first industry-relevant compliance management research agenda for IS researchers.

Keywords: Regulatory Compliance, Business Information Systems, Empirical Study.

1 Introduction

Compliance involves ensuring that business processes, operations and practice are in accordance with a prescribed and/or agreed set of norms. Even though predominantly viewed as a burden by organisations [1], failing to comply is no longer an option [2, 3]. Non-compliance may not only result in the possibility of losing customers and damaging reputation, but can also lead to legal action. A number of corporate scandals - Enron, WorldCom (USA), HIH (Australia), Societe Generale (France) and, most recently, Satyam (India), to name a few - have exhibited this situation.

In addition, there is a general consensus that there will be an upsurge of regulatory reform as a response to the events that led to the global financial crisis. Developing strategies to manage inevitable regulatory shifts that emerge from government and global reactions to the financial crisis is going to be high on corporate agendas in the coming years. This situation is bound to put pressure on organisations already struggling with the economic downturn.

B. Pernici (Ed.): CAiSE 2010, LNCS 6051, pp. 251–265, 2010.

With compliance expectations on the increase, evidence suggests that organisations experience difficulties in managing compliance expectations and are increasingly concerned with high costs associated with compliance [4]. Indeed, spending on compliance is steadily increasing [5, 6]. With each new introduced regulation new challenges arise [7-9]. The inevitability of coping with compliance pressures identifies a need for new IT and IS solutions to compliance management and denotes a need for evolution of current IT and IS approaches such that they are better able to support the fast-changing regulatory compliance management field. Any developed solutions, to be adequate, need to be informed by industry practice and expert advice. The development of solutions in this domain without input from industry experts and professionals will only serve to increase compliance management spending without delivering on the promise of suitable IT and IS tools to alleviate compliance management problems.

In this paper we take steps to address this need through an empirical study with compliance management professionals. The main goal of the reported study is to investigate compliance management issues and challenges faced by industry, as perceived by compliance management experts, to investigate where IS research can contribute and how IS tools should evolve to support industry. We conduct a gap analysis of the perceived challenges with existing research in IS and identify a set of issues and challenges that should drive the future agenda of IS researchers.

2 Approach and Methodology

To extract issues and challenges, we utilise semi-structured interviews. Interviews are an established and popular means of carrying out qualitative enquiry in the fields of social sciences. We use a semi-structured interview type to provide the opportunity for participants to think about the challenges in compliance management and reflect on and relate their experiences [10]. The interview team consisted of two experienced empirical researchers, one with the role of the main interviewer and the other with a support role of note taking and further probing. The interviewers' domain knowledge and expertise with the interview method is an essential element for success in these semi-structured interviews.

2.1 Data Sampling, Participants and Protocol

The nature of the study led us to adopt a deliberately selective sampling approach to participant involvement. We were motivated to ensure that participants had extensive experience in the domain and would therefore provide an insightful and accurate reflection of the state of compliance management in practice. To that end, we enlisted the help of the Australasian Compliance Institute (ACI) and obtained a selection of experienced contacts with insight into both the mature and immature stages of compliance management in organisations. Eleven participants were invited to participate and all eleven agreed with no incentives present for participation. Accordingly, eleven Australian compliance management experts were interviewed in the last quarter of 2007. Typical roles interviewed were those of senior compliance management advisors and consultants in large organizations that provide both advisory and auditing services in the context of regulatory compliance. Among the eleven, nine possess more than 10 years of experience in the field and the other two have five and seven years of experience in the field respectively.

The semi-structured interview protocol[1] was designed and pilot tested to elicit free flowing information from the interviewees. The protocol consisted of high level questions that captured the experience of the interviewee, their opinions relating to regulations and related challenges, as well as their experiences and observations of challenges in compliance management practice. The questions were open-ended in nature so as not to bias the interviewees. The researchers relied on probing to identify specific challenges when an interviewee indicated a limitation they had experiences.

The protocol included three main sections. The first section aimed to establish the context of the interview session. This section consisted of demographic inquiry such as role, experience and organisation description. The second section asked interviewees to provide opinions about heavily regulated industry sectors, what compliance responsibilities existed in their organisation and their awareness and experience with current IT- and IS-related tools in use. The third section of the protocol aimed to obtain explanation about the compliance-related factors - such as issues, hurdles and solutions. Interviewees were asked to identify these factors in relation to customers, regulations and solutions. In addition, participants were also encouraged to incorporate examples during elaboration of key points.

2.2 Data Analysis

All interviews were transcribed, annonymised, and analysed using a multi-coder approach and NVivo as the supporting tool. The multi-coder approach was used to reduce coder bias in the analysis of the text and multiple rounds of analysis were carried out for each transcription. As the study was exploratory in nature, all factors emerged from the interview data. To facilitate the exploration of factors, an initial meta-level node structure was derived from the interview protocol – *viz.* responses related to regulatees, regulations and solutions. This structure was used and expanded upon each time a new issue, challenge, problem, regulation, etc, was identified.

The detailed coding, using the initial node structure as the basis, was conducted in the first round by a third researcher, in a few iterations of the full transcripts so as to capture the most detail. After each iteration, the coding node structure and associated interview data was examined and revised before the next iteration of interview data coding took place. The final coding and the resulting expanded coding structure were then independently reviewed and re-coded separately by two researchers who identified the initial node structure. Following this individual analysis, the two researchers then jointly discussed each node and its contents and refined the coding structure to reduce overlaps and refine aspects of some identified issues (i.e. split nodes). The researchers then jointly again analysed each transcript to ensure that all relevant detail was captured and correctly codified.

[1] Due to space limitations the interview protocol is omitted from this paper. The interview protocol is available from the authors on request.

3 Results

In the following we present an in-depth discussion of the main challenges identified in the interview sessions. Based on the analysis of the expert interviews, Figure 1 shows the number of participants referring to each regulation and number of references made respectively. Among all regulations referred to by the participants, Anti-Money Laundering (AML) was the most frequently referred to and also the only one discussed by all the participants. This finding is perhaps not surprising given the recent introduction of the regulation. Australian Standards was the second most frequently discussed, followed by Financial Services Regulation (FSR), Organisational Health and Safety (OHS), Trade Practices Act, Corporation Act and Sarbanes-Oxley (SOX).

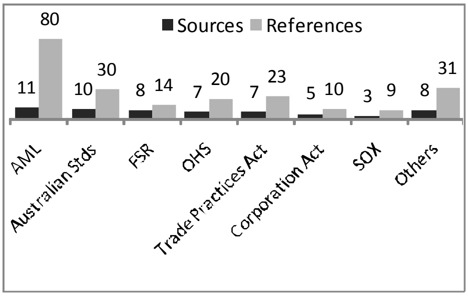

Fig. 1. Regulations Identified by Experts

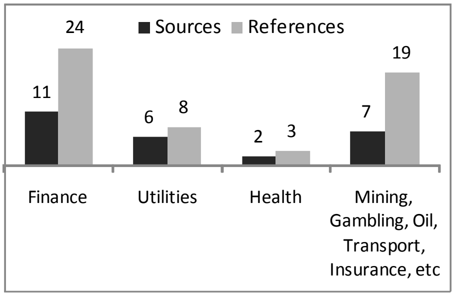

Fig. 2. Industry Sectors Identified by Experts

In terms of the industry sectors that are considered to be highly regulated, Figure 2 similarly depicts the number of references/participants regarding identification of the most regulated markets. The experts indicated that the financial sector is the most heavily regulated industry - addressed by all the participants with a total of 24 supported references. This finding correlates the earlier indication of a strong AML focus.

After understanding the landscape of various sectors and their compliance requirements, we turned to investigating the challenges that organisations face in their compliance management activities. The discussion of the identified challenges and expert opinion is provided in the next sub-sections, logically separated into challenges and problems related to customers (i.e. regulatees), regulations and solutions. We precede the discussion of the challenges with the table showing the challenges and the

Table 1. Customer Factors

FACTORS	SOURCES	REFERENCES
Lack of Compliance Culture	10	46
High Cost	9	43
Lack of Efficient Risk Management	9	37
Difficulties in Creating Evidence of Compliance	8	29
Lack of Perception of Compliance as a Value-add	8	25
Lack of Understanding of its Relevance to Business	6	12
Lack of Communication among Staff	4	4

number of participants who identified them, as well as the frequency of the identifications (number of references). Tables 1, 2 and 3 present factors relating to customers, regulations, and solutions respectively.

3.1 Factors Relating to Customers

Lack of Compliance Culture. All the participants indicated that culture plays a vital role in inculcating compliance. One of the participants indicated: "… compliance doesn't mean a thing if the culture isn't right within the organisation." Culture refers to the overall compliance culture of the organisation, which involves employees' perspective towards the organisation, what the organisation stands for, its customers, investors, regulators and fellow colleagues [11]. A good culture, though difficult to achieve [12] can promote a positive attitude towards legal compliance activity at all levels within an organisation.

Several issues relating to culture were identified from the expert interviews. The core issues related to top level management beliefs and mindset. The board often sees compliance as one of the least value-added activities for the organization. Consequently, the operational level often lacks guideline and advice, which further results in naive and inexperienced compliance approaches among employees. This situation is made worse because compliance officers often have little influence in the management board of organisations. A participant indicated that: "… they need to get top level buy in and then try – if there's no buy in from senior management, it's not going to run." This issue has also been highlighted by KPMG [13], where it is suggested that balancing risk and controls with business improvement begins with the identifications of priorities and opportunities from a high-level, or so called "top-down" perspective.

Similarly, the corporate mindset is affected directly by belief of employees. One participant stated: "… Even if it's a black letter law, it's still a mindset. … Like you don't want to know that you're reporting valid financial information to the market…" This statement illustrates that some organisations lack willingness to accept compliance activities within business operations. Further, one of the participants pointed out that some organisations tend to allocate junior (those who "either had nothing to do in projects once projects finished or were being managed") and "non-star" resources to risk and compliance section. The experts also indicate that some organisations are reluctant to provide IT/IS tool support for compliance staff. Another culture related issue is the lack of pro-active culture that leads to low compliance achievement for the organisation. The problem is propagated to the mindset of the organisation, in which "compliance is done for the sake of compliance instead of compliance for the sake of good business."

High Cost. Cost of compliance is one of the vital issues that make organisations hesitant to get a compliance framework in place [14]. According to experts, one of the compliance cost-related issues is the size of the company, especially affecting small to medium sized companies (SMEs). Due to human resource and financial capital limitations, these companies are found to struggle to put a compliance framework in place - "… the smaller you are, the less capacity you've got to even feel confident about it because you haven't got the skills either in capital, technology, or finance to actually put that control framework in place" (interview data). In other words, despite differences in organisational size, small companies those have an equivalent "complexity function" to that of large enterprises have to pay for an equivalent compliance frameworks without an equivalent budget.

Lack of Efficient Risk Management. Another issue recognised by participants is that of reluctance to allocate adequate resources to manage the risks, while being aware that those risks exist. As one of the participants stated: "… in a risk identification sense, you identified your risks and you said we've got to look at these, but then you didn't resource to actually address that…"

On the other hand, it is also possible that the issue is linked to the mindset of the employees. The employees might see that it is too risky to be a compliance officer: "… There's personal liability attaching to everything now. If you look at money laundering legislation for example, I've got clients who say "Who'd want to be the money laundering reporting officer? You could go to jail…" Complicating this issue is the fact that regulatory risk is not transferable (e.g through purchasing insurance). In risk management, there are several approaches that organisations use in dealing with risk: reduce, mitigate, accept or transfer the risks [15, 16]. Organizations have to rely on an effective approach to reduce regulatory risks given that the consequence of failing to report breaches is severe.

According to the findings, organisations tend to see compliance as being one of the risk management frameworks - this situation is found to be consistent with general organisation structure [13]. Developing effective risk management begins with a clear understanding of an organisation's appetite for risk [17]. However, this is difficult to achieve. It depends on the ability of the risk assessment framework to keep up with legislative and regulatory changes. It is a nature of legislations and regulations to change in order to capture changes and growth in business. Risk assessment, on the other hand, needs to be monitored and updated on an ongoing basis so that it can capture those changes. As a result, organisations are faced with high monitoring costs, which, in turn, prevent them from having effective risk management.

Difficulties in Creating Evidence of Compliance. One of the experts highlighted "…got to do the right thing and not only they have to do the right thing, they have to demonstrate that they're doing the right thing." This revealed that organizations need for effective techniques to demonstrate their business conformity to obligations. Other experts also agreed, e.g. "… People need systems to improve the internal efficiency to be able to demonstrate that compliance and document stuff." These views confirm the need for an appropriate control framework to facilitate internal controls, especially incident recording and reporting.

Lack of Perception of Compliance as a Value-add. Many organisations see little (or no) value-add of compliance controls being embedded in their business processes. Those organisations, having documented their business activities, argue that they see no returns for the time consuming and expensive documentation: "The business never gets anything back, so there's no value provided back to the business from the data that's collected and then heaven forbid, stuff gets reported to the board without the business knowing about it." Moreover, some organisations believe that risk and compliance frameworks add complexity to business: "risk and compliance actually makes it harder because they can't visualize the business so they get attracted to adding systems into the processes that serve their purposes but don't serve businesses purposes." Furthermore, some organisations claim that the only business benefit derived from compliance frameworks is that they avoid getting fined by regulators.

Lack of Understanding of its Relevance to Business. Organisations face difficulties in relating obligations to their business; that is, which rule(s) is/are relevant to which business objective(s) and activities. To overcome such difficulties, it is required that regulations and legislations are interpreted in relation to, and mapped to, business processes by experts who deeply understand both the legal and the operational aspects of the organisation. Experts also recognise this issue, e.g. - "The rules and obligations are not the problem; it's the organisation's capacity to understand how it needs to run its business to achieve its objectives." As a result of lack of understanding on how to correctly embed rules and obligations in their business, organisations are found [18].

Lack of Communication among Staff. Based on the interview data, the lack of efficient communication channels within the organisation is one aspect that prevents an organisation from having an effective compliance framework in place is. Once there is a change in obligation, organisations find it complicated to communicate the change: "… you can't really have people in a business unit just by themselves … So they have to be linked somehow and another situation is the fact that if they are not linked into that business unit somehow, they tend to be left … they don't participate in team meetings, people sort of isolate them and that's a real danger …." In addition, another communication issue is associated with compliance monitoring, where risks and compliance problems that are identified in business operations are not reported back to the board.

3.2 Factor Relating to Regulations

Frequent Changes in Regulations. The fact that regulations, legislations, government rules and laws regularly change means that organisations struggle to keep up with the new requirements [13, 19, 20]. Updates of existing compliance frameworks and internal controls to comply with the new obligations are a key problem, as highlighted by one of the participants: "… because of the rapid change around regulatory reform, we're finding organisations becoming more inefficient in trying to meet these obligations."

Table 2. Regulations Factors

FACTORS	SOURCES	REFERENCES
Frequent Changes in Regulations	7	12
Legislation Weaknesses	6	11
Inconsistencies	5	8
Overlap in Regulations	3	7

Legislation Weaknesses. According to the experts, the challenges related with legislations were mostly found in principle-based legislation. Principle-based legislation puts the approach on meeting the legal obligations to be decided by the regulated party. Although this approach allows organisation to be creative in applying the legislations, it exposes the organisation to the risk of making inappropriate interpretations of legislation.

Inconsistencies. The problem of consistent application of common standards across several jurisdictions (states and territories) is recognized as one of the central problems of regulation [21]. As a result, some organisations choose to comply with those inconsistent regulations, which generate negative consequences, particularly compliance cost [22]. Not only are regulations inconsistent domestically, but also internationally. For example, "… most countries impose regulation for those entities that they regulate, not only in the home jurisdiction, but offshore, and if, let's take Deutchse Bank, if the German authorities impose restrictions or regulatory frameworks on Deutchse Bank, they've got to apply it here in Australia. That may or may not be consistent with domestic law here."

Overlap in Regulations. One of the main challenges with regulations is the problem of duplication. In the Australian context, for example, the duplication is mainly between the states and the Commonwealth **[21]**, due to multiple legal parties. Organisations are affected because they are required to demonstrate evidence of compliance multiple times. As one expert exemplifies: "… I kept on seeing that I was going to organisations exactly the same obligations coming through in five different pieces of legislation and then the people out of the business pushing back saying 'But I've already answered this in relation to …"

3.3 Factor Relating to Solutions

Lack of Holistic Practices. Even if a high-quality compliance framework is in place, organisations can be stagnant in terms of improvement if the framework is not properly managed. It is believed that compliance must be cascaded through every layer in the organisation, starting with clear direction from the top, and then deployed appropriately at each level [23]. The relationship between the two is captured by a quote of one of the participants: "… governance is around the right behaviors, appropriate risk management, corporate social responsibility, ethics, managing, reporting to stakeholders, …,."

Table 3. Solutions Factors

FACTORS	SOURCES	REFERENCES
Lack of Holistic Practices	5	8
Lack of IT Support/Tools	11	103
Lack of Compliance Knowledge Base	7	35

Lack of IT Support/Tools. Despite the rising investment from software vendors and entrepreneurs in governance, risk and compliance (GRC) software products, organisations are struggling to correctly identify the tools and its suitability to their requirements. The features identified by Gartner [24] - reporting, dash-boarding, remediation management, business process modelling, risk management and support for multiple regulations across multiple business units - were mostly also identified by the participants. The participants also highlighted that lack of IT support/tools are related to usability and comprehensiveness of the tools, the supported learning and training program, tools features such as monitoring and reporting, self-assessment, management, newsfeed, alert, and updates. Participants highlighted a need for tools relating to reporting/monitoring, self assessment, newsfeeds/alert, learning and management. Moreover, participants also stressed that tools should include the ability to deliver not only regulatory compliance but also business benefits.

In particular, participants emphasized the important role played by monitoring tools in compliance management: "… you can't monitor customer's transactions manually, … there's millions of transactions." It is also important that monitoring tools be able to oversee all business operations so that anomalies can be traced back to the source of the problem if a breach occurs. This requirement leads to the need of breach reporting and incident recording functionality. Furthermore, as one participant pointed out – "…reporting tools should be able to effectively filter out irrelevant data and provide meaningful reports to the audit committees". So that instead of acquiring an external audit firm, organisations can obtain internal audit management tools that can provide regular audits, and keep the risk library small.

Lack of Compliance Knowledge Base. Generally, the advisory program provides the necessary guidance to handle complex regulatory requirements. Experts highlighted that advisory related challenges centered on the development of compliance knowledge base, linking regulations to business processes, and the reliance to comprehensive guidelines and frameworks. Many consulting firms offer such a service including of course - the Big Four - i.e. KPMG, PricewaterhouseCoopers, Ernst & Young and Deloitte Touche Tohmatsu. According to the experts, some organisations that already have compliance frameworks in place continue to have difficulties in carrying out tasks properly as a result of lack of comprehensive knowledge. Advisory services contribute in this space by assisting on compliance strategies, and to overseeing and evaluating the overall performance of compliance outcomes. One of the main foci of the above is to define an appropriate training program. The experts confirmed the lack of effective training programs.

Issues related business processes were also identified – in particular linking or embedding controls/regulations to processes – and are focused on advisory services that analyse existing processes wrt. relevant regulations.

4 Information Systems Research on Compliance Management

In [8], the first comprehensive snapshot of the development and focus of compliance management related research in the Information Systems (IS) discipline is presented. The study includes papers from premium Information Systems journals (as promoted by the Association for Information Systems), and some additional popular journals in the discipline. Aiming to introduce a well-informed research agenda, we further extend the report to include reputed conferences in the discipline. Our target is to further identify the existing IS research that contributes to solving compliance management problems.

The results are presented within a framework that was developed to establish relevance and analyse the contributions[2]. Within this framework, case study and exploratory papers are differentiated from papers that provide a solution to a compliance management related problem.

Table 4 shows the breakdown of papers relevant to compliance management and their source of publication. Out of 19637 articles, 232 articles matched the context. Although the number is relatively low, the roles of IS or IT as enablers of regulatory compliance have increased year by year (details below).

Table 4. Sources and Frequency of Publication

SOURCES (Journals)	**TOTAL**	**Relevant Articles**	**%**	**SOURCES** (Conferences)	**TOTAL**	**Relevant Articles**	**%**
CAIS	659	16	2.4	BPM	189	7	3.7
BPMJ	336	5	1.5	ACIS	906	28	3.1
JAIS	158	2	1.3	CAiSE	346	9	2.6
JI&M	502	4	0.8	ICIS	959	14	1.5
CACM	2178	17	0.8	PACIS	1025	14	1.4
JISR	199	1	0.5	AMCIS	3822	46	1.2
EJIS	382	2	0.5	HICSS	4517	49	1.1
MISQ	281	1	0.4	ECIS	1489	17	1.1
				ER	400	2	0.5

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 - 188 (81%) of the articles are case study/exploratory articles and 40 (17.2%) are solution articles. However, there are four (1.7%) 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.

Furthermore, we were interested to determine the emergence of compliance management research in Information Systems publication outlets. The breakdown of compliance management research per year of publication is shown in Figure 3.

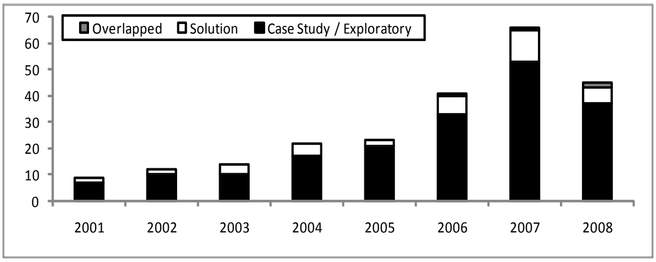

Fig. 3. Distribution of Article per Type per Year

[2] 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".

The figure shows an upward trend in compliance management research in Information Systems, with a spike of publications in 2007. We posit that this finding is in line with the increased focus on SOX Act of 2002 and also an early focus on HIPAA, given the lag of publishing in the Information Systems discipline. Prior to this event, little literature on compliance management exists, despite some other regulations having already been proposed.

Following this analysis, we carried out further classification for the articles that were classified as solution articles. This classification involved 44 solution articles and also 4 articles that contain both (case study and solution) discussion. These articles were reviewed to identify the focus of the solution in relation with challenges identified in section 3. The study reveals that 29 out of 44 articles offer a preventive (before-the-fact) solution, 14 offer a detective (after-the-fact) solution, while the remaining (one) offers both solutions.

5 Research Agenda for Compliance Management

In this section we present an analysis of the gaps between expert opinion and current status of IS literature with regard to published Information Systems compliance management solutions. A summary is provided in Table 5.

Due to space limitations it is not possible to discuss the contributions of the 44 papers identified as contributing to compliance solutions. The actual solutions presented in the papers vary substantially. Some of the papers, for example, [25] addressed detective types of solution and introduced the Hippocratic Database Compliance Auditing component, which facilitates audits in E-health records.

In [26] the researchers introduce the 'compliance by design' approach that proposes a compliance regimen with a preventative focus. Similarly [14] present a high level view of regulatory compliance through a policy-based framework for integrating regulatory compliance tasks with business processes.

We observe that the growing focus on technical aspects of compliance, is balanced by research on business or management aspects. For example, [27] detailed the development and application of an evaluative data model for ISO 9000 compliance. On the call to facilitate compliance with HIPAA, [28] introduce a framework that provides a useful way of identifying and analysing the training needs of organisations with diverse user communities and continuous change.

As shown in Table 5, the solution challenges, i.e. lack of holistic practices, lack of IT supports/tools, and lack of compliance knowledge base, have received most attention from the IS researchers with 13, 14 and 10 matching solutions respectively. This demonstrates that the focus of IS research community is slanted towards providing solutions either in form of best practices, automation, or guidelines. The analysis also exposed that regulatee challenges *viz.* high cost, lack of efficient risk management, and lack of perception of compliance as a value-add; despite receiving high attention from the experts, have not yet been addressed adequately. Difficulties in evidencing compliance, although addressed in research in 2002 and 2003, shows drought from 2004 to 2008. This is contrary to experts' opinion, which stresses difficulties in evidencing compliance and the need for appropriate incident recording and reporting mechanisms.

Table 5. Industry Challenges vs. Current Research Focus

	INDUSTRY CHALLENGES	SOLUTIONS (by year)							
		2001	2002	2003	2004	2005	2006	2007	2008
Customers	Lack of Compliance Culture							1	1
	High Cost								
	Lack of Efficient Risk Management								
	Difficulties in Creating Evidence of Compliance		1	1					
	Lack of Perception of Compliance as a Value-add								
	Non-proactive								
	Lack of Understanding of its Relevance to Business						1	2	1
	Lack of Communication among Staff								
Regulations	Frequent Changes in Regulations			1	1				1
	Legislation Weaknesses								
	Inconsistencies								
	Overlap in Regulations								
Solutions	Lack of Holistic Practices				4	1		6	3
	Lack of IT Support/Tools	2	1	1	1	1	5	1	3
	Lack of Compliance Knowledge Base			2			3	4	1

In terms of solutions for regulations related challenges, very few solutions can be found and all (three) relate coping with frequent changes. Other challenges i.e. legislation weaknesses, inconsistencies, and overlap in regulations are not addressed, which is not surprising as this is more in the legal arena and controlled by government agencies, legislation authority or standardisation bodies.

The review of the related papers as well as the interview transcripts allowed us to extract key aspects where IS research can create results and value for organizations in meeting their compliance obligations. In the discussion below, we highlight the key challenges that need attention from the IS research community and indicate how the challenges relate to addressing industry challenges:

First and foremost, there is an urgent need for proper **benchmarking studies** to help address the challenge of *high cost*. Particularly for SMEs, there is high cost and great difficulty in **measuring the adequacy of controls** for principles based regulations where the onus is on the organization to design an appropriate compliance regimen. Benchmarking and best practice studies will allow improvement of controls effectiveness, a reduction of costs, and an improved potential to deal with resistance to change through demonstrating methods used by others. Such additional knowledge can further help alleviate the perception of *legislation weaknesses* in principles based regulations and consequently promote regulation acceptance.

In a related manner, there is also a need for investigation of **process reference models** relating to various regulations. A focus on the development of such reference models and the study of the impact of the use of such models in organizations (i.e. impact on compliance management spending, frequency of breaches, etc) is largely missing in Information Systems research. The development of proven reference models, however, may significantly lessen the cost of compliance management in organizations.

The *culture of compliance* is ingrained in the daily rituals of each of the firm's employees, including senior management, who must learn to lead by example [12]. There is a clear lack of Information Systems research on **organisational behaviour**. In particular we see a need for investigation of how IT and IS tools can be used to incentivize employees to 'do the right thing' and adapt their practices. There is also a need for the development of relevant IT and IS tools that can help facilitate employee training for compliance management, promote *communication among staff* and increase organizational capacity to manage its *compliance knowledge base*.

How the compliance (and *risk*) factor interrelates with the operations of business units is understudied, with only a small number of researchers working on the **conceptualisation of compliance and risk** requirements per se let alone their interrelationships with business processes and business activities. A comprehensive and well-grounded conceptual model for compliance and risk is needed.

Further to the point above, tools and methods are needed to **annotate, enhance, analyse and simulate business models** with compliance and risk modeling elements. This will facilitate better coordination between an organization's compliance and business functions and help employees understand *compliance value* and *business relevance*.

Although reporting and monitoring tools of high sophistication are available, there is little development towards tools that provide **specialized solutions in monitoring and analysing** compliance related data (partly due the absence of any generic conceptual models for GRC), thus causing big problems for organisations required to create *evidence of compliance*. Accordingly, we see a need for affordable IT and IS tools that facilitate compliance management self-audits and compliance monitoring activities in general. Furthermore, there is also a clear need for tools that facilitate the identification of non-compliance processes with respect to a given regulation.

Although *frequency of change*, as well as *inconsistency* and *overlaps* in regulations is beyond the realm of IS research, studies to understand the **impact of regulation changes** (inconsistencies and overlaps) can promote better understanding of the cost of compliance and allow business to lobby for regulatory reform where needed. Multi disciplinary research is warranted in order to cover legal, business and IT aspects. From an Information Systems perspective, there is a need for solutions that can filter out updates that are not relevant to a given organization or industry sector, thus reducing the amount of information that the organization has to process in order to update or assess their compliance management initiatives.

In conclusion, this paper presents insights into the issues and challenges perceived by experts involved in managing compliance. In addition, we present a snapshot of IS research activity since 2001 and contrast it against the challenges identified by industry experts. The findings, and related discussion, are expected to be beneficial to the research community in particular as they communicate the opinion of industry experts that should be taken into consideration when undertaking research in the field, thereby resulting in research activity that has the potential to impact and contribute to practical problems faced by organizations.

One of the limitations of our work, beyond the geographic limitation to Australia, is the focus on experienced consultants. The consideration of views from various roles in organisations will be a complement to the study in the future. Further we will undertake a review of contributions from computer science research (in particular research in the database community) as anecdotal evidence indicates that there have been substantial contributions with respect to e.g. solutions leading to automated monitoring and analysis of business /transactional data.

Further limitations of the work relate to the qualitative aspect of the study. Qualitative studies in particular can suffer from subjectivity in data analysis. In our study, through using multiple coding rounds, together with multiple coders, we have taken measures to ensure objectivity of the analysis.

References

1. Lu, R., Sadiq, S., Governatori, G.: Compliance Aware Business Process Design. In: ter Hofstede, A.H.M., Benatallah, B., Paik, H.-Y. (eds.) BPM Workshops 2007. LNCS, vol. 4928, pp. 120–131. Springer, Heidelberg (2008)
2. Anon, J.L., Filowitz, H., Kovatch, J.M.: Integrating Sarbanes-Oxley Controls into an Investment Firm Governance Framework. The Journal of Investment Compliance 8, 40–43 (2007)
3. Pershkow, B.I.: Sarbanes-Oxley: Investment Company Compliance. The Journal of Investment Compliance 3, 16–30 (2003)
4. Bace, J., Rozwell, C., Feiman, J., Kirwin, B.: Understanding the Costs of Compliance. Gartner Research. Gartner, Inc. (2006)
5. McGreevy, M.: AMR Research Finds Spending on Governance, Risk Management, and Compliance Will Exceed $32B in 2008. AMR Research, Inc. (2008)
6. Reilly, K.: AMR Research Finds Spending on Sarbanes-Oxley Compliance will Remain Steady at $6.0B in 2007. AMR Research (2007)
7. Robinson, K.T., Hawkins, R.W.: Investment Company and Investment Adviser Compliance Programs: New Requirements in a Changed Regulatory Environment. The Journal of Investment Compliance 4, 14–19 (2004)
8. Syed Abdullah, N., Indulska, M., Sadiq, S.: A Study of Compliance Management in Information Systems Research. In: The 17th European Conference on Information Systems (ECIS 2009), Verona, Italy (2009)
9. Turner, R., Florio, C.D.: Investment Management Compliance: The Dawn of A New Era? The Journal of Investment Compliance 4 (2005)
10. Kramp, M.K.: Exploring Life and Experience through Narrative Inquiry. In: Marrais, K.d., Lapan, S.D. (eds.) Foundations for Research: Methods in Education and the Social Sciences, pp. 103–121. Erlbaum, Mahwah (2004)
11. Australian Competition & Consumer Commission: Trade Practices Compliance Programs. Commonwealth of Australia (2008)
12. Morton, J.C.: The Development of A Compliance Culture. The Journal of Investment Compliance 6, 59–66 (2005)
13. KPMG: The Compliance Journey: Leveraging Information Technology to Reduce Costs and Improve Responsiveness. KPMG International (2006)
14. Kharbili, M.E., Stein, S., Markovic, I., Pulvermüller, E.: Towards a Framework for Semantic Business Process Compliance Management. In: GRCIS 2008, Montpellier, France (2008)
15. SAI Global Research: Risk and Compliance in Australia: The Issues and Trends as Seen by Practitioners (2008)

16. Sadiq, S., Indulska, M.: Driving Compliance through BPM. The University of Queensland (2008)
17. Abrams, C., Känel, J.v., Müller, S., Pfitzmann, B., Ruschka-Taylor, S.: Optimized Enterprise Risk Management. IBM Systems Journal 46, 219–234 (2007)
18. Governatori, G., Milosevic, Z., Sadiq, S., Orlowska, M.: On Compliance of Business Processes with Business Contracts. ITEE Technical Report. The University of Queensland, Brisbane (2007)
19. Karagiannis, D., Mylopoulos, J., Schwab, M.: Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act. In: 15th IEEE International Requirements Engineering Conference (RE 2007), pp. 315–321 (2007)
20. Liu, Y., Müller, S., Xu, K.: A Static Compliance-checking Framework for Business Process Models. IBM Systems Journal 46, 335–361 (2007)
21. Wilkins, R.: The Problems of Duplication and Inconsistency of Regulation in a Federal System. In: Grabosky, P., Braithwaite, J. (eds.) Business Regulation and Australia's Future. Australian Institute of Criminology, Canberra (1993)
22. Harmer, R.: Current Views on Compliance & Governance. Rob Harmer Consulting Services (2004)
23. Paul, S.: Demand for Governance, Risk and Compliance Products on The Rise. The Hindu Business Line (2008)
24. Caldwell, F., Eid, T.: Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms. Gartner Research. Gartner, Inc. (2008)
25. Agrawal, R., Grandison, T., Johnson, C., Kiernan, J.: Enabling the 21st Century: Health Care Information Technology Revolution. Communications of the ACM 50, 35–42 (2007)
26. Sadiq, S., Governatori, G., Naimiri, K.: Modeling Control Objectives for Business Process Compliance. In: Alonso, G., Dadam, P., Rosemann, M. (eds.) BPM 2007. LNCS, vol. 4714, pp. 149–164. Springer, Heidelberg (2007)
27. Kim, H.M., Fox, M.S., Sengupta, A.: How to Build Enterprise Data Models to Achieve Compliance to Standards or Regulatory Requirements (and share data). Journal of the AIS 8, 105–128 (2007)
28. Davis, C.J., Hikmet, N.: Training as Regulation and Development: An Exploration of the Needs of Enterprise Systems Users. Information & Management 45, 341–348 (2008)