Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2011 Proceedings | Australasian (ACIS)

2011

Governance, risk and compliance (GRC): Conceptual muddle and technological tangle

Catherine Hardy
University of Sydney, catherine.hardy@sydney.edu.au

Jenny Leonard
University of Sydney, jenny.leonard@sydney.edu.au

Governance, risk and compliance (GRC): Conceptual muddle and technological tangle

Catherine Hardy
Jenny Leonard
Business Information Systems
University of Sydney Business School
catherine.hardy@sydney.edu.au
jenny.leonard@sydney.edu.au

Abstract

The concepts of governance, risk and compliance are not new. However, the label 'GRC' has more recently gained traction in research and practice. Given the growing interest in GRC it is timely and important to reflect upon developments, as the literature is now peppered with a wide array of views to the extent that the term risks being misunderstood in theory and practice. This paper summarises and critiques the GRC literature for the purpose of revealing: the diversity of ambitions, assumptions and ambiguities that require questioning in conflations of governance, risk and compliance; and gaps in present research agendas. Grounding our argument on the critique of the literature we open up discussion of alternative perspectives and identify their possible contribution to the study of GRC. Moreover we argue that Latour's (2005) concept of 'panorama' has the potential to fruitfully broaden the notion of GRC.

Keywords

GRC, enterprise systems, risk, control, panorama

INTRODUCTION

The concepts of governance, risk and compliance are not new. However, the label 'GRC' has more recently gained traction in the business environment, largely due to technology vendors, analysts and consultants (Marks 2010). High profile corporate collapses and frauds, the recent global financial crisis, natural disasters and increasing regulatory compliance obligations have been put forward to advance the business case for GRC in terms of assisting top management meet demands for greater accountability and better manage reputational risks and financial losses through a more comprehensive and unified approach. Attention has been directed at technology platforms (Racz et al. 2010c) designed for the purpose of improving oversight of corporate governance, incorporating "financial reporting compliance, enterprise risk management (ERM) and associated audits" (Caldwell 2010). In addition support for information technology (IT), operational and industry-specific requirements, as well as other capability areas such as privacy, data protection, business continuity management, continuous assurance/continuous monitoring and performance management have been recognised (Caldwell et al. 2009).

Despite broad recognition of the GRC label few enterprises have succeeded in integrating GRC activities (Caldwell et al. 2009; Racz et al. 2010a, 2010b). Resistance to change, complex integration processes and a lack of available expertise were identified in a recent KPMG survey (2010) as the greatest barriers to successful convergence. Currently the literature is peppered with a wide variety of GRC views creating confusion as to what GRC actually means. Does this suggest that a major change is required in terms of how governance, risk and compliance are conceptualised and managed because of new possibilities enabled by new information technologies, or is GRC just a new fashion or marketing ploy?

The aim of this paper is to revisit the notion of GRC, reflecting upon developments in the literature in terms of what it means and review concepts and research that have come to characterise this developing idea. Our review focuses on GRC definitions and frameworks in the scholarly and practitioner literature. We also examine research studies and the theories and methodologies being applied. Our objective is to improve understanding of GRC and question the ends it serves by revealing ambiguities in terms, conflations of ideas and assumptions that underlie the different ways the concept has been used. When the literature is regarded in this way, we see that the study of GRC lacks theoretical cohesion. We offer alternative perspectives and identify possible contributions to GRC research. In particular, we argue that Latour's (2005) concept of 'panorama' has the potential to fruitfully broaden the notion of GRC.

METHODOLOGICAL APPROACH

The paper primarily focuses on frameworks and research studies published since 2009. We build on a literature review of 107 sources (published between 2004-2009) conducted by Racz et al, (2010a). The Racz et al (2010a) paper was analysed and used as a starting point for structuring further searches based on the guidelines suggested by Webster and Watson (2002 p.xvi), that is: a keyword search using the Summon™web-scale discovery service on the terms "governance, risk and compliance/GRC;" review of relevant books (Tarantino 2008); and review of web sites and publications of key professional groups active in the area (Open Compliance Ethics Group (OCEG) http://www.oceg.org/; Information Systems & Control Association (ISACA) http://www.isaca.org/; Institute of Internal Auditors (IIA) http://www.iia.org), market research (eg. Gartner) and professional services organisations. The literature review process followed more of a critically reflective process (see Boell and Cezec-Kecmanovic 2011) with the aim of identifying ambiguities, approaches and directions in GRC research. This contrasts to a more "systematic review" which emphasises the literature identification and selection process (Boell & Cezec-Kecmanovic 2011).

GRC AS CONCEPT: MEANING AND SCOPE

The notion of GRC is used in a descriptive (see Table 1) and normative (see Table 2) sense. In a descriptive sense GRC is viewed as a system (OCEG 2009), an approach (Marks 2010; Racz et al.2010a) and an objective for improving governance (Proctor & Caldwell 2011) through or while managing risks and complying with laws and regulations. It serves multiple purposes including meeting stakeholder expectations, improving performance and ensuring ethical conduct. In a normative sense GRC is viewed as a model or framework for "scoping and approaching a GRC research project" (Racz et al. 2010a) or to assist organisations "better understand" (Frigo & Anderson 2009), implement and manage "a GRC system or some aspect of that system" (OCEG 2009).

Common understandings of GRC, represented in "scientifically derived" (Racz et al. 2010a) and "best practice" (OCEG 2009) definitions promote the same basic idea and are general in scope. Interestingly, the version offered by the Open Compliance and Ethics Group (OCEG), a not for profit organisation with Charter members including organisations such as SAP, PWC, Ernst & Young, Deloitte, Microsoft and Dell (amongst others), has, in a relatively short period of time, become a major referent point in research and practice. The OCEG guidance sets out the eight "integrated components" and "universal outcomes" of a "high-performing GRC system" that is striving for "Principled Performance®." Further, Racz et al. (2010a) and the OCEG (2009) view GRC as more than what the acronym represents, consisting of a range of activities and processes incorporating: strategy and business performance management; risk management; compliance; internal control; corporate security; legal; information technology; business ethics; sustainability and corporate social responsibility; quality; management; human capital and culture; audit and assurance; and finance. (OCEG 2009, 8-9).

While the concepts of governance, risk and compliance have been meshed into a single view, GRC is intertwined with other terms such as accountability, ethics, internal control and assurance, representing what Drori (2006, p.100) described in the context of the broader governance field as a "discursive package." Each concept has been borrowed from and considered separately in the areas of governance, risk management and compliance management; the latter only more recently viewed by some (Bace et al. 2010) as a dedicated business function rather than a function of other business areas such as legal or records management. Varying conceptions and logics in these different disciplinary and professional fields have been "absorbed" and "infused" in the GRC term permeating the work of IT, accounting, assurance, legal and business professionals. Further, the term GRC has, similar to what Drori (2006, p.112) observed in the governance literature, "various, different and decoupled meanings [that] coexist in the same terminology because the notion and the term has acquired a general and religious like following." For example Marks (2010) presents an internal audit perspective in terms of providing assurance over the organisation's governance, risk management and internal control processes. Control is viewed as a part of governance, risk and compliance whereas compliance is an aspect of risk management. Finally, varying labels and conceptions of control (eg. internal controls, financial controls, IT controls, management control, organisational control), governance (eg. corporate and IT) and performance (eg. ethical and efficient) were raised under the universalistic claims of GRC.

This conceptual muddle is further reduced predominately to characterisations of GRC as an 'integrated' view. Even when the integrated term was not explicitly mentioned in the definition, it was frequently mentioned as an important feature that often coincided with the terms enterprise or organisation-wide. Further the term 'integration' is conceptualised and employed differently in the GRC literature. For example, OCEG (2009) describes an integrated view as "applying a common vocabulary, approach and ideally technology infrastructure to GRC processes." Marks (2010) described GRC "convergence" as "fundamentally about the fragmentation of risk management and compliance." Racz et al. (2011) viewed the concept of GRC integration in five ways: with business processes, particularly in terms of continuous monitoring; with performance management, and risk management as the link; as integrated software on a single platform; the centralisation of GRC "relevant information" consisting of enterprise content management and risk management, and, finally, in analytics and

reporting across the various "disciplines" or domains of GRC. Hence integration is revealed as a significant issue yet ambiguous, a goal but represented in many ways. This raises questions, as to whether an enterprise wide GRC integration can actually be achieved given, as suggested by Dechow and Mouritsen (2005) that "in its instantiation integration has to be seized and can be taken in many directions from as many different positions."

GRC AS TECHNOLOGY

Significant attention is directed at GRC technologies in the literature, represented by multiple GRC technologies (see for eg. Heiser 2010), vendors and multi-service solutions (see for eg. Caldwell 2010). Attempts at classifying GRC technologies (see for eg OCEG 2009; Racz et al. 2011) have proved difficult for a number of reasons. Firstly, there have been a number of acquisitions (Caldwell 2010) and partnerships (eg. Deloitte and IBM, Protiviti and SAP, BWise and CapGemini, PricewaterhouseCoopers and CA) in the GRC marketplace; each from similar and different traditions. These partnerships alone have implications for the implementation of GRC technologies; a point we return to later on in this paper. Second, the label 'GRC' is used in the context of point or stand alone solutions such as continuous control monitoring and records retention technologies as well as in the context of a common platform, the latter usually referred to as an enterprise GRC platform. The enterprise GRC platform is commonly viewed as a way to "unify complex architecture" as well as enabling a common reporting capability "through the integration of technologies and information supporting multiple GRC activities" (Caldwell 2008).

Classification schemes for GRC platforms are also problematic in terms of the labels used and meanings attached to terms. For example, the OCEG (2009) classifies "technology modules" into nine "technology arenas" consisting of: Corporate Governance (CG); Business Intelligence (BI); Business Process Management (BPM); Enterprise Resource Management (ER); Human Resource Management (HRM); Enterprise Risk Management (ERM); Enterprise Content Management (ECM); Assurance and Audit Management (AAM); and Security Management (SM). In addition, the modules are categorised within "technology levels" described as business applications, GRC specific applications and infrastructure. Caldwell (2008) from Gartner classified audit management, compliance management, risk management, policy management and remediation management as GRC functional categories which can be integrated with business applications, business intelligence, specialised GRC applications, enterprise content management and controls automation and monitoring. Racz et al. (2010a) refers to business rules management, business process management and enterprise content management as methodologies. Finally, Proctor and Caldwell (2011) from Gartner make the distinction between GRC management (GRCM) solution providers and GRC controls. The former refers to functions that "span" finance, legal, IT and operational domains incorporating: the establishment of policies, assessment of risk to performance and compliance; assessment of the effectiveness of controls; the remediation of risk and control deficiencies; assurance processes; and dashboards and reporting functions. GRC controls refer to "domain specific needs" in terms of Finance GRC (eg. SOD in ERP systems); IT GRC (eg. identify & access management); Operations GRC (eg. greenhouse gas emissions monitoring); and Legal GRC (eg. record retention policies, automated fraud monitoring). AMR Research (cf Racz et al. 2011) prior to being acquired by Gartner, made a further distinction using the label 'GRC execution capabilities' to refer to access controls and identity management, business process controls, audit testing tools and data security products and 'GRC applications' for business processes specific to particular regulatory or industry requirements such as environment, health and safety and IT risk management. The third category 'GRC management software' is similar to the Gartner description.

PREVIOUS RESEARCH STUDIES IN GRC

Summarising across the limited number of studies, as set out in Table 3, most conceive of GRC as existing in a determinant relationship with its environment and technology. The environment, consisting of risk management and compliance requirements, presents imperatives for organisations to adopt an enterprise GRC 'solution' for the purpose of improving performance, through better business processes, control designs and reporting. From this somewhat mechanical like position, surveys of the literature and "GRC professionals" in online business network groups and industry workshops have been conducted to construct "scientifically derived" definitions, models and understandings of technology use. Further, these studies have primarily been conducted in German speaking countries. Whilst these studies have provided insights into practice, they assume that there are similar goals and organisational forms and black-box technology by limiting the investigation into software use rather than how it came to be in particular and changing socio-technical environments. Further, although GRC is often conceptualised as multi-dimensional there is limited evidence of it being empirically operationalised into multi dimensions, thereby confounding different elements in the research design. Finally, there is further need for theoretical development. We return to this point later in our discussion.

Table 1 Descriptions of GRC

Author	Description	Scope	Stakeholders	Key elements & descriptions			
				Governance	Risk Management	Compliance	Other
OCEG (2009)	"…system of people, processes and technology that enables an organisation to: understand and prioritize stakeholder expectations; set business objectives while optimising risk profile and protecting value; operate within legal, contractual, internal, social and ethical boundaries; provide relevant, reliable and timely information to appropriate stakeholders; and enable the measurement of the performance and effectiveness of the system."	IT enabled GRC Management & Operational Governance, risk & compliance	BOD Executive Mgt Auditors IT managers Risk managers Compliance managers	"… culture, values, mission, structure & layers of policies, processes and measures by which organisations are directed and controlled… includes but is not limited to the activities of the Board…"	"… the systematic application of processes and structures that enable an organisation to identify, evaluate, analyse, optimise, monitor, improve or transfer risk while communicating risk & risk decisions to stakeholders…"	"… act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies."	"**Principle performance®** is the outcome of a clear articulation of an enterprise's objectives … and application of the GRC methods …" **Internal control** – specify the policies, procedures and practices that guide org. efforts to achieve objectives. **Assurance** – maintain stakeholder confidence that the organisation has appropriate governance, risk management & compliance capabilities. **Human behaviour & conduct** – understanding what motivates human behaviour.
Krey (2010)	"an **approach** that addresses … the **establishment of business rules** [and] … **how those rules are integrated** into sensible organisational structures, embedded into … business processes of the organisation, communicated and monitored for compliance"	IT GRC Management IT governance	Executives BOD	IT Governance (Based on CobiT): strategic alignment; value delivery; resource mgt; performance mgt.	"transparency about the significant risks to the enterprise and embedding of risk mgt responsibilities into the organisation."	"conform to a specification or policy, standard or law that has been clearly defined for the healthcare sector by the canton or the federal government."	
Marks (2010)	"how an organisation understands stakeholder expectations and directs and manages activities to maximise performance against those expectations, while managing risks and complying with applicable laws, regulations and obligations." [influenced by OCEG]	IT enabled GRC Management GRC convergence	Consultants/ nalysts Software vendors BOD/ Executive Int Auditors	"limits governance to activities performed by the board [while] governance component of GRC" broader.	Not separately defined	Not separately defined	"internal auditing provides assurance over the organisation's governance, risk mgt and internal control processes. In 'GRC' controls are "included in each of the three" whereas compliance is an aspect of risk management.
Racz et al. (2010a)	"an integrated, holistic approach to org-wide governance, risk and compliance ensuring that an org acts ethically correct and in accordance with its risk appetite, internal policies and external	IT GRC & IT enabled GRC **Overall GRC:** business ops **IT GRC:** InfoSec	GRC professionals	Described as a "core subject" - not separately defined	Described as a "core subject" -not separately defined	Described as a "core subject" - not separately defined	Integrated Holistic Organisation wide Alignment Strategy People

Author	Description	Scope	Stakeholders	Key elements & descriptions			
				Governance	Risk Management	Compliance	Other
	regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness."	IT compliance; IT & data governance; risk mgt; IT revision.					Technology Processes Ethical acts Efficiency & effectiveness
Proctor & Caldwell (2011)	"GRC is neither a project nor a technology, but a corporate objective for improving governance through more-effective compliance and a better understanding of the impact of risk on business performance."	IT enabled GRC Mgt & Operational	Business mgrs Risk mgt mgrs Compliance mgrs	"The process by which policy is set and decision making is executed."	"The process for preventing an unacceptable level of uncertainty in business objectives [and] … ensure … business processes and behaviours remain within tolerances…"	"The process of adherence to policies and decisions [derived from] from internal directives, procedures and requirements, or external laws, regulations, standards and agreements."	
Wiesche et al. (2011)	"…integrated governance, risk and compliance perspective on mgt controls for accounting."	IT enabled GRC Management AIS & control	Auditors, Compliance Vendors	Not separately defined	Not separately defined	Not separately defined	

Table 2: GRC frameworks

General Framework Attributes					Framework Design	
Name	Author/ Published	Target audience	GRC Area	Purpose/ Goal	Key Concepts/ Elements	Description/Guidance on Use
An Enterprise GRC Framework and Architecture	Rasmussen (2009)	Internal auditors	GRC architecture	Identify and define GRC factors that influence software adoption and implementation decisions.	**Unified:** provide a "unified and enterprise-integrated view of… risk and compliance." **Automated: "**deploy technologies [to] … automate risk and compliance processes and enforce controls" **Integrated:** "an architecture … to facilitate management and reporting across the enterprise." **End-to-end**: "end to end management of risk and controls across identities, infrastructure and information in the GRC architecture and business processes." **Easy to use**: "users … must have information and process management presented in a meaningful way." **Flexible**: "business is dynamic, and GRC applications and information must evolve as the business evolves."	
Strategic Governance, Risk & Compliance Framework	Frigo & Anderson (2009)	Finance Org	Governance, risk and compliance	Help organisations "better understand GRC."	**Functions:** Legal; IA; Compliance; Safety; IT; Finance SOX **Enterprise risk policy & appetite** – board & executive **Risk Assessment** **Emerging risk identification** **Risk/Control Monitoring (KRIs)** **Value Creation & Preservation -** outcome	GRC functions share common goals of creating & preserving stakeholder value (primary goal of enterprise & strategic risk mgt). Each risk & control function is "part of a fully integrated effort with a common goal to manage the organisation's risks." Functions identify and leverage common processes, technologies & knowledge "under a common governance umbrella, the org's risk mgt policy"
GRC Capability Model "Red Book" 2.0	OCEG (2009)	Business	Governance, risk & compliance	To provide a "comprehensive guideline" to "anyone	**8 integrated components:** Organise & oversee; Assess & Align; Prevent & Promote; Detect & Discern; Respond & Resolve; Monitor & Measure; Culture & Context; Inform & integrate. **8 universal outcomes:** Achieve business	• Components "embody integrated Elements of a high-performing GRC system" and "operate in a somewhat sequential manner" • Universal system outcomes are "the expected and measurable results of a high-performing GRC system"

General Framework Attributes					Framework Design	
Name	Author/ Published	Target audience	GRC Area	Purpose/ Goal	Key Concepts/ Elements	Description/Guidance on Use
				implementing & managing a GRC system or some aspect of that system."	objectives; Enhance organisational culture; Increase stakeholder confidence; Prepare & protect the organization; Prevent, detect, & reduce adversity; Motivate & inspire desired conduct; Improve responsiveness & efficiency; Optimise economic & social value	• Elements embody "a number of related Practices in a high-performing GRC system.
Frame of reference for integrated GRC	Racz et al. (2010a)	Researchers	Governance, risk and compliance	Frame of reference to support "scoping and approaching a GRC research project."	**Core subjects**: Governance, Risk and Compliance **Each subject has four components**: Strategy, Processes, Technology, People **Rules:** Risk appetite, Internal policies, External regulations **Characteristics:** Integrated, Holistic, Org-wide **Objectives:** Ethically correct behaviour, Improved efficiency and effectiveness	"The subjects, their components and rules are …merged in an integrated, holistic and organisation-wide manner – aligned with the (business) operations that are managed and supported through GRC. In applying this approach, organisations long to achieve the objectives of GRC … of any of the elements involved."
GRC comparison model	Proctor & Caldwell (2011) [Gartner]	Business & IT managers	GRC mgt	To structure GRC goals, functions and requirements	**Four GRC domains:** Finance; IT; Operations; Legal **GRCM technologies:** common to all four domains **GRC controls**: highly specialised domain specific **Corporate governance**: finance and legal domains **Operational risk**: IT and operations	Domains represented along a continuum. Mgt capabilities at centre **GRCM**: activities for establishing policies to support governance; risk assessment; control assessment; remediation; auditing; reporting. **GRC controls**: Finance, IT, Operations, Legal

Table 3: Previous research studies in GRC

Author	Objective	Business case (B) &/or Research Imperative (R)	Focus	Approach and perspective	Empirical domain/ Participants	Key findings
Krey (2010)	Provide an "overview of the common IT governance models already used in the healthcare sector" and assess whether they meet requirements.	**B:** Need for an "integrated and comprehensive approach for the governance of IT and its resources…" in response to the introduction of the Swiss Diagnosis Related Groups (DRG) in 2012. **R:** Establish what IT governance models are currently being used in practice.	IT GRC	Survey	23 Swiss hospital chief information officers	• ITIL for IT service management most commonly used. 8% of hospitals have or will be adopting CobiT, ISO-17799 (now 27001/27002) or a proprietary framework. • Board/Snr mgt's understanding of IT risk limited. • Majority planned response to compliance on a requirement-by-requirement basis. Only 9% of hospitals believe they have an 'integrated approach to compliance…"
Racz et al. (2010a)	To provide a "frame of reference for research of integrated GRC"	**B&R**: The concept behind the acronym (GRC) "has neither been adequately researched, nor is there a common understanding among professionals."	IT GRC & IT enabled GRC	Survey of literature Survey - "groups" in networks XING and LinkedIn.	107 articles (2004-2009). 131 "GRC professionals:" 42% consulting; 18% vendors; 16% work in orgs; 11% auditors; 5% research institutions; 4% other	• Lack of research on GRC • Definition "derived rigorously in a scientific manner …" • Frame of reference - high-level abstraction of GRC [that] "does not visualise the massive complexity of GRC" [but] assists in structuring research.
Racz et al. (2010b)	Construct an "integrated process model for high-level IT GRC management."	**R:** Integration of IT GRC not adequately researched."	IT GRC mgt	Design science – process model Literature review	N/A	Process model for IT GRC management proposed based on: ISO/IEC 38500:2008; COSO ERM framework; Rath & Sponholz (2009).

Author	Objective	Business case (B) &/or Research Imperative (R)	Focus	Approach and perspective	Empirical domain/ Participants	Key findings
Racz et al. (2010c)	Evaluate how "GRC and GRC software are perceived and applied in large enterprises."	**B:** Importance of IT enabled GRC increasing, but challenges remain in terms of integrating GRC activities. **R**: Limited scientific research on integrated GRC in general and the use of GRC software in business.	GRC technologies	N/A Online survey	48 professionals holding positions mainly concerned with governance, risk management and compliance. Global companies in German-speaking countries.	• Integrated GRC more advanced at the organisational level than process or technology • Half used "GRC" software. In house preferred to "standard solutions." • Integrated GRC reports to management are used, but more than half considered them to be insufficient.
Krey et al. (2011)	Provide a classification scheme for IT governance frameworks	**B:** An "IT GRC framework for [Swiss] healthcare" to assist "hospital strategy" **R**: A classification of existing IT governance frameworks required to assist in mapping requirements.	IT governance	Prescriptive Survey of frameworks	N/A	Description & explanation of a classification scheme.
Racz et al. (2011)	Determine what is "state-of-the-art GRC software according to the software industry, and how should scientific research deal with it?"	**B:**Technology vendors a major driver in the GRC domain with many offerings. **R:** Limited research into the architecture and functionality of GRC software. In the first instance need to identify the software used under the "umbrella of GRC."	GRC technologies	1. Review of existing research on GRC software classifications & frameworks. 2. Survey – 10 questions (via email)	8 out of 27 companies who were providers of "integrated GRC mgt suites:" CA, IDS, Scheer, MetricStream, Protiviti, SAP, Thomson Reuters, Wolters Kluwer & Paisley (subsequently acquired by Thomson Reuters). Vendors of point solutions were excluded.	• vendors share a common understanding of GRC • vendors view ERM as part of GRC or interconnected with "overlapping methodologies that share certain processes and technologies." • diverse perceptions of GRC functionality • scope of software frameworks vary strongly • vendors agree on the benefits delivered through integrated GRC suites to a large extent. • Technology architectures of vendors mainly differ in their degree of integration • Integration a common theme across five GRC technology trends for the future.
Kominars (2011)	Identify factors that influence a "successful IT GRC implementation" & features of IT solution that add value to the internal audit function.	**B:** The complexity of the business environment requires that current methods of internal audit be extended to examine controls and processes that "span not only business processes and operations, but also supporting technology."	IT GRC	Prescriptive	N/A	**Adoption factors**: inexpensive; easy to use; easy to adapt; easy to integrate; accessible from anywhere; highly secure **Technical features** of IT GRC solution: Single & centralised repository (standards, regulations, policies & audit/control templates); Integration of assessments & audit procedures; Automated linkage to test results; Master scheduling; Assignment of personnel to audits; Audit issue life cycle management; Dashboards & reports
Wiesche et al. (2011)	"Appraise the impact of IT on accounting by understanding value drivers of AIS such as GRC IS"	**R:** Limited understanding in the management accounting literature of the impact of IT on management controls.	GRC IS as AIS	Organisational control theory Grounded Theory Interviews	14 "experts" auditors, consultants, governance, users, compliance, IT and risk mgrs attending a GRC workshop in Germany.	Four value drivers of GRC IS: Control automation; Control coherence; Early warnings; Management resilience

DISCUSSION OF FINDINGS AND IMPLICATIONS

The growing GRC literature represents a diversity of ambitions, concepts, technologies and increasingly a research program. In summary, the ambitions of GRC initiatives appear threefold. Firstly, it undertakes to improve performance through an *integrative* and *organisational-wide* approach to governance, risk and compliance and in doing so minimise and mitigate against past business failures. Secondly, these new possibilities for GRC are achievable through 'new' *enterprise technologies*. Thirdly, GRC is an enticing and ambitious project advocating greater *accountabilities* and *Principled Performance®*.

Making sense of GRC developments is challenging as the basic conception of GRC, as revealed above, is overly general and contentious. Further, there are currently only a limited number of empirical studies and theoretical views. To address these issues further empirical research is required particularly in a range of organisational and international contexts. In addition, GRC research could extend the range of theories and adopt methodologies designed to uncover taken for granted assumptions by drawing from the fields of governance (eg. Drori 2006), risk management (eg. Bhimani 2009; Power 2009), management control (eg. Berry et al. 2009; Dechow & Mouritsen 2005) and accounting information systems (eg. Granlund 2011; Rom & Rohde 2007). Specifically, we argue that GRC is limited at the design level in three separate and related areas and propose alternate theoretical perspectives to assist in: broadening the conceptual foundation by introducing Latour's (2005) concept of "panorama;" developing understanding of the consequences of GRC in terms of transparency and accountability; exploring the influence (or not) of GRC technologies on an organisation's integration capabilities to facilitate more 'effective' governance, risk and compliance processes.

GRC as a "panorama"

The review of GRC as set out particularly in Tables 1 and 2 reveals a multiplicity of views ranging from the very broad, such as a "corporate objective" to a specific function or control, such as Finance SOX, as well as frameworks for defining the general activities encompassed by GRC. It is not unreasonable to argue that various conceptualisations are not unexpected because, beyond high-level classifications, governance, risk and compliance activities will vary in different contexts. For example, risk management activities in financial services will not be the same as in a manufacturing context. Hence GRC may simply viewed as a new 'topography' for framing governance, risk and compliance activities. We argue similar to Latour (2005, 185-186) that the framing activity of GRC itself should be given more attention to be convinced that "connections exist" as the "zoom" (nesting the micro, meso and macro) used to 'smoothly order' GRC matters "may wane and wax pretty fast." In doing so, we propose that Latour's (2005, 187-189) concept of *panoramas*, may provide a useful way to broaden the conceptual foundations of GRC as it demonstrates a "desire for wholeness and centrality." As the metaphor suggests, we see *everything* and *nothing* like the images projected on the walls in the Omnimax cinema rooms. Hence the GRC 'Big Picture' becomes just that a picture, whereby questions regarding the simultaneity of governance, risk and compliance in organisations are considered in terms of for example: who is projecting and in which room (eg. technology vendors, consultants, new compliance imperatives or fraud); through which medium (eg. frameworks and GRC software); to what audience (eg. internal auditors, business or IT managers); and for what purpose (eg. GRC management, GRC controls, IT governance). Latour (2005, 189) argues that these social wholes while ambiguous need to be studied because "through their many clever special effects they offer a preview of the collective" and "no matter how much they trick us, they prepare us for the political task ahead." This awaits further investigation.

GRC outcomes: better information and ethical accountabilities

GRC objectives broadly promoted are effectiveness, efficiency, better information and ethical accountabilities. Yet, as Racz et al. (2010c) identified there is currently limited theoretical understanding of supposed benefits. Vague demands for better information and calls to "establish policies for information accountability, retention, archiving, review and destruction" (Caldwell et al. 2009) remain un(der) explained and un(der) explored. Further, different possibilities (Roberts 1991), limits (Messner 2009) and styles (Ahrens 1996) of accountability may also create different understandings of and ambitions for GRC. Investigation of this moral imperative is required as involvements with technologies (such as GRC) may address ethical problems as well as be products of such technological involvements (Smith 2003) such as OCEG's registered trademark of "Principled Performance" where our discussion turns.

GRC as enterprise and enterprising technologies

The integrated and enterprise or organisation-wide view of GRC is problematic. Such "ambitions" of representing the organisation as an integrated whole have been questioned in other areas. For example Dechow and Mouritsen (2005) found that ERP systems did not provide a "global visibility" but created "blind spots" (deleted certain organisational representations) and visibilities in a "lot of trading zones" (organisational

representations are shifted from accounting based to non-financial representations). Power (2009) argued that the "programmatic dreams" of enterprise risk management (ERM) exposed organisations to the "risk management of nothing" as its "thin simplification" was inadequate to "reproduce domain-specific complexity" and points to the business continuity management field for developing insights into 'interconnectedness.' Ciborra and Hanseth (2000, 3) argued the difficulty in achieving control and the inevitability of technologies designed to strengthen governance capabilities creating a resistance to control.

Notwithstanding the attention directed at GRC technologies and the range of offerings, there is still limited understanding about how they are configured in organisations, how they are actually used for GRC purposes, what the technology actually does and more importantly doesn't, for example, are there certain kinds of compliance not possible particularly in changing regulatory environments? Our review of SAP GRC documentation for example was unclear about the implications of different configurations. These are important questions as it is the systems of classification that "form a juncture of social organisation, moral order and layers of technical integration" (Bowker & Star 1999, 33). In addition, GRC and its designs have been strongly influenced by software vendors and their partnerships with professional advisory organisations. This has implications in terms of how they shape the GRC implementation process, risk frameworks, control designs and for 'GRC professionals' at the individual level and functional areas. Does this suggest in following Power's (2009) view of ERM, that GRC is really an "entrepreneurial" activity or market opportunity "explicitly in the service of wealth creation." Or does it represent an interpretive struggle of institutional entrepreneurs, particularly in the context of the OCEG group, where institutions are formed as meanings become shared and taken for granted (Hardy & Maguire 2008). Such matters await further investigation

CONCLUSION

This paper reviewed the growing GRC literature. The diversity of meanings, ambitions and technologies that were revealed presented a state of ambiguity for future research. We found existing conceptions of GRC limited and proposed an alternate way of framing GRC by drawing on Latour's (2005) panorama concept. Further we identified two additional limitations of GRC at the design level and proposed alternative theoretical perspectives inspiring a number of key research directions within the GRC domain. We hope that this paper provides the impetus for further debate.

REFERENCES

Ahrens, T. 1996. "Styles of Accountability," *Accounting, Organizations and Society*, 21(2/3), pp. 139-173.

Bace, J., Morency, J.P. and Caldwell, F. 2010. "Understanding the Components of Compliance." Gartner Report ID: G00209580.

Berry, A.J., Coad, A.F., Harris, E.P., Otley, D.T. and Stringer C. 2009. "Emerging themes in management control: A review of recent literature," *The British Accounting Review*, 41(1), pp. 2-20.

Bhimani, A. 2009. "Risk management, corporate governance and management accounting: Emerging interdependencies," *Management Accounting Research*, 20, pp 2-5.

Boell, S.K., and Cezec-Kecmanovic, D. 2011. "Are Systematic Reviews Better, Less Biased and of Higher Quality?" ECIS 2011 Proceedings. Retrieved on 5 July 2011 from http://aisel.aisnet.org/cgi/query.cgi

Bowker, G.C. and Star, S.L. 1999. *Sorting Things Out, Classification and Its Consequences*, USA: MIT Press.

Caldwell, F. (2008). "The Enterprise Governance, Risk and Compliance Platform Defined", Gartner Report ID: G00155196.

Caldwell, F. 2010. "Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms." Gartner Report ID: G00206382.

Caldwell, F., Wheatman, J. and Bace, J. 2009. "Predicts 2010: Comprehensive Governance, Risk and Compliance Remains Elusive." Gartner Report ID:G00172945.

Ciborra, C.U. and Hanseth, O. 2000. "Introduction." In Ciborra, C.U and Associates (eds), *From Control To Drift, The Dynamics of Corporate Information Infrastructure,* New York: Oxford University Press, pp1-11.

Dechow, N. and Mouritsen, J. 2005. "Enterprise resource planning systems, management control and the quest for integration, " *Accounting, Organizations and Society*, 30, pp 691-733.

Drori, G.S. 2006. "Governed by Governance: The New Prism for Organizational Change." In Drori, G.S., Meyer, J.W. and Hwang, H (eds), *Globalization and Organization, World Society and Organizational Change*, New York: Oxford University Press, pp. 91-118.

Frigo, M.L. and Anderson, R.J. 2009. "A strategic framework for governance, risk and compliance," *Strategic Finance*, 90(8), pp.20,22,61.

Granlund, M. 2011. "Extending AIS research to management accounting and control issues: A research note," *International Journal of Accounting Information Systems*, 12, pp 3-19.

Hardy, C. and Maguire, S. 2008. "Institutional Entrepreneurship." In Greenwood, R., Oliver, C., Sahlin, K and Suddaby, R. (eds), *The SAGE Handbook of Organizational Institutionalism,* London: Sage Publications Ltd, pp 198-217.

Heiser, J. 2010. "Hype Cycle for Governance, Risk and Compliance Technologies." Gartner Report ID: G00205229.
Kominars, H.M. 2011. "IT GRC aims for performance gains," *Internal Auditor* 68(2), pp.63-65.
KPMG International. 2010. "The convergence challenge, Global survey into the integration of governance, risk and compliance." Retrieved 10 November 2010 from http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Pages/The-convergence-challenge-Global-survey.aspx
Krey, M. 2010. "Information Technology Governance, Risk and Compliance in Health Care – a Management Approach." In 2010 Developments in E-systems Engineering Conference Proceedings, pp 7-11.
Krey, M., Harriehausen, B., and Knoll, M. 2011. "Approach to the Classification of Information Technology Governance, Risk and Compliance Frameworks." In 2011 UKSim 13th International Conference on Modelling and Simulation Proceedings, pp 350-354.
Latour, B. 2005. *Reassembling the Social, An Introduction to Actor-Network-Theory*, USA: Oxford University Press.
Marks, N. 2010. "Defining GRC," *Internal Auditor*, February, pp 25-27.
Messner, M. 2009. "The limits of accountability," *Accounting, Organizations and Society*, 34, pp. 918-938.
Open Compliance and Ethics Group (OCEG). 2009. GRC Capability Model "Red Book" 2.0. Retrieved 29 October 2010 from http://www.oceg.org/resource/red-book-20-basic-member-edition
Power, M. 2009. "The risk management of nothing," *Accounting, Organizations and Society*, 34, pp 849-855.
Proctor, P.E. and Caldwell, F. 2011. " A Comparison Model for the GRC marketplace, 2011-2013." Gartner Report ID: G0210517.
Racz, N., Weippl, E., and Seufert, A. 2010a. "A Frame of Reference for Research of Integrated Governance, Risk & Compliance (GRC)." In Communications and Multimedia Security, 11th IFIP TC 6/TC11 International Conference, CMC 2010 Proceedings, Berlin: Springer, pp 107-116.
Racz, N., Weippl, E., and Seufert, A. 2010b. "A process model for integrated IT governance, risk and compliance management." In Databases and Information Systems, Proceedings of the Ninth International Baltic Conference 2010 Riga, University of Latvia Press, pp 155-170.
Racz, N., Panitz, J.C., Amberg, M., Weippl, E. and Seufert A. 2010c. "Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from A Survey Among Large Enterprises." ACIS 2010 Proceedings, Paper 21. Retrieved on 7 May 2011 from http://aisel.aisnet.org/acis2010/21
Racz, N., Weippl, E., Seufert, A. 2011. "Governance, Risk & Compliance (GRC) Software – An Exploratory Study of Software Vendor and Market Research Perspectives." Proceedings of the 44th Hawaii International Conference on System Sciences.
Rasmussen, M. 2009. "An Enterprise GRC framework," *Internal Auditor,* 66(5), pp. 61,63,65.
Roberts, J. 1991. "The Possibilities of Accountability," *Accounting, Organizations and Society*, 16(4), 355-368.
Rom, A. and Rohde, C. 2007. "Management accounting and integrated information systems: A literature review," *International Journal of Accounting Information Systems*, 8, pp 40-68.
Smith, A. 2003. "Do You Believe in Ethics? Latour and Ihde in the Trenches of the Science Wars (Or: Watch Out, Latour, Ihde's Got a Gun)." In Ihde, D. and Selinger, E. (eds), *Chasing Technoscience, Matrix for Materiality*, Bloomington: Indiana University Press, pp 182-194.
Tarantino, A.G. 2008. *Governance, Risk, and Compliance Handbook,* Hoboken, NJ: John Wiley & Sons, Inc.
Wiesche, M., Schermann, M., Kremar, H. 2011. "Exploring the Contribution of Information Technology to Governance, Risk Management, and Compliance (GRC) Initiatives." ECIS 2011 Proceedings, Paper 4. http://aisel.aisnet.org/ecis2011/4

ACKNOWLEDGEMENTS

The authors would like to acknowledge Professor John Roberts, Chair of the Accounting Discipline at The University of Sydney for kindly sharing his idea of the 'panorama' in the BIS Discipline Research Day, April 2011. We would also like to thank the anonymous reviewers for their comments.

COPYRIGHT