Which is better for embedding risk management in higher education quality assurance: ISO 31000 or the COSO framework?

Fernando F. Padró
University of Southern Queensland

Abstract

Purpose: The focus of this paper is two-fold: [1] to explain risk management (RM) from an enterprise (ERM) or institutional perspective and from a regulatory (RRM) perspective and [2] to explore issues pertinent to choices involved in determining whether to adopt RM and how to implement it from the single college or university standpoint and/or from a sector viewpoint in relation to existing quality assurance (QA) and quality control (QC) practices.

Design/Methodology/Approach: This paper is a conceptual analysis of the RM literature as it applies to higher education. RM is a developing practice in higher education and RM itself is a maturing field with transdisciplinary interests.

Findings: There are different RM models that are utilized by different business and industry sectors. Two models are dominant, the COSO Framework and the ISO 31000 standard, RRM is practiced in Australia and the UK is about to use RRM as the key component of its higher education oversight process. In the USA, the practice of RM is more indirect and voluntary based on following the dicta set forth in the Sarbanes-Oxley Act of 2002.

Practical implications: QA frameworks in higher education (HEQAs) are noticing the development of RM and, as the most recent development in QA, may want to consider adopting RM. There are a number of considerations in pursuing the adoption and implementation of RM at the institutional and sector levels and this paper highlights key considerations. Six concerns and seven questions are identified and discussed to help frame the decisionmaking process relating to RM adoption.

Originality/value: There is little in the literature regarding the adoption, implementation, and use of RM in higher education. There is also a scant amount of articles and studies on how to integrate RM into QA schemes, especially in higher education. This paper provides an introduction to both these discussion points.

Keywords: COSO, Higher Education Evaluation, HEFCE, ISO 31000, Risk management, Sarbanes-Oxley, TEQSA

Introduction

This paper is an introductory and macro level attempt to discuss the implications of adopting risk management (RM) as part of higher education quality assurance (HEQA) schemes as RM is becoming more common either as an enhancement or as a replacement system. That this is occurring is not surprising as risk has become a force for political mobilization, often replacing earlier approaches to referencing and interpreting qualitative norms (Adam & van Loon, 2005). The approach taken here is one information sharing to better understand what RM brings to quality assurance practice, as it seems to have become the current evolutionary next step in quality practice as exemplified in the Malcolm Baldrige National Quality Award (MBQNA). This exchange is meant to identify issues and implicitly provide a structured approach to considerations that inform the decisions related to its adoption, particularly as it can relate quality assurance (QA) activities to the background in order to decrease the burdensomeness of regulatory compliance adds to higher education institutions (HEIs) in general. For example, recent developments in higher education regarding RM are found in the UK where the Higher Education Funding Council for England (HEFCE) intends to replace regular institutional reviews currently performed by the Quality Assurance Agency (QAA) in favor of a risk-based inspection system (Grove, 29 June 2015). On the other hand, retrenchment in Australia to its initial regulatory risk framework under the Tertiary Education Quality Standards Agency (TEQSA) suggests a reduction of quality assurance (QA) practice to concentrate on a risk-based review process.

RM remains a minority practice, but getting more attention. In addition to Australia and the UK, it is practices to a lesser, arguably more indirect extent, in the USA through the National Association of College and University Business Officers' (NACUBO – 2003) recommendation to adopt practices identified in the *Sarbanes-Oxley Act of 2002* (SOX) which has links to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) risk framework (Langevoort, 2006). Canada too has recently embarked on adopting risk assessment (RA) practices that are considered to be synonymous with RM (Marsh Canada LTD, 2012) while New Zealand continues to build on organizational RM capacity (Tertiary Education Commission, 2014). Attempts at finding out about RM practices in other countries usually, if found, provide links to the UK, Australia, or the USA. Some other national quality assurance agencies also seem to practice elements of RM, but specific discussions link either back to HEFCE or TEQSA to provide the basis of their activities.

Arena, Arnaboldi, and Azzone (2010) point out that RM's fluidity in linking managerial and control processes tends to be overlooked by hierarchical models emphasizing regulation, which brings to the fore the question of what models/frameworks to adopt. The rationale behind the adoption of RM is found in Australia's Baird Report from 2010:

> Risk needs to be better identified at entry into the sector and a range of indicators need to be used that go to the heart of whether the provider will be able to operate successfully now and in the future. This assessment of risk should guide whether the provider gains entry to the sector, and it should be used to test and scrutinise providers already through the gateway (p. vi).

Various financial scandals in the 1980s and 1990s placed an importance on risk management, especially in the UK and USA that has led to its application and embedding within managerial schemes (Power, 2007; Dionne, 2013). The modern understanding of risk is based on decisions occurring under conditions of uncertainty that can be identified, quantified and measured probabilistically, and thus managed (Zachman, 2014). There tends to be a cultural divide between the use of qualitative and quantitative data although there are attempts to bridge the cultures and these are seen as providing benefits to organizations (Jasanoff, 1993; Zachman, 2014). The development of big data generates an attraction to the sue of quantitative modeling for decisions; however, there is the *caveat* of over-reliance on models at the expense of judgement when it comes to identifying and assessing risk (O'Shea & Krischanitz, 2013).

There likewise is a divide on how to look at and define risk, which creates the challenge of which framework to adopt when adapting it to an existing HEQA scheme or creating a new one. The two more popular frameworks that are in place approach risk from a threats perspective; yet, only one treats risk from an opportunities viewpoint as well.

RM in higher education is still somewhat of an unknown. Knowledge of it is distant and incomplete. Its language may be comfortable for campus administrators and regulators, but it is not necessarily so for academics and professional staff not directly involved in financial matters. As a result, the logic of its application and its capacity to engage with reciprocal ongoing interactions with other, pre-existing organizational processes (Arena, Arnaboldi, & Azzone, 2010) may not be as clear and implementation of RM could be incomplete, routinized, and superficial without much attached meaning to the users. Also, there is a pervasive concern that risk is not a managerial fad (Birnbaum, 2000) or that its calculus immunizes decisionmaking against the perception of failures (Luhmann, 1993). This paper therefore broaches RM from an introductory perspective. The discussion primarily centers on the two more widely renowned RM frameworks – COSO's framework and the ISO 31000 Standard and the options they provide HEQA agencies and HEIs.

The next section provides a generic background of RM's utility from regulatory and organizational theoretical perspectives. After that comes a presentation of Australia's HEQA scheme that is equally based on a risk framework, institutional standards, and a national qualifications framework (Padró & Kek, 2013). This is followed by a description of the COSO framework and the ISO 31000 Standard and, finally, a discussion of which model best fits an HEQA scheme or HEI.

Background

HEQA's evolution is trending toward regulatory compliance and how HEIs manage the uncertain world. Higher education's environment continues to become more complex because of the challenges emanating from stakeholder expectation preference for the achievement of specific outcomes (access, affordability, employment, workforce development, commodification), a changing definition of the role of HEIs and the systems in which they are housed (from critical thinking, exploration, and personal development to workforce training and marketization), and policy steering and regulatory compliance oversight demands based on a trade-off between autonomy and assurance of quality practice and meeting government expectations. The challenges reflect Huber and Daft's (1987) characterization of a complex environment: *numerosity*, *diversity*, and *interdependence*. There is *numerosity* because of the number of relevant actors involved with higher education

(internal and external). *Diversity* refers to the differences among the markets served, in higher education's case the different markets being the different employers (business and industry), governments (who define what the obligations are and the truth-telling processes – Foucault, 2010), and other social agents who make claims to what HEIs provide. *Interdependence* is indicative of the impact that increased information flow and analysis that can be gleaned from analytics, for example, represent in terms of institutional action. This complexity in the environment begets different forms of uncertainty, especially about the state of the exogenous environment, affecting what is noticed, ignored, strategic postures and actions related to current and future state of the sector, managing institutional responses/actions, and the risks associated with enacted institutional action (Milliken, 1987; Weick, 1995; Courtney, Kirkland, & Viguerie, 1997; Riesch, 2012). Compounding the problem for organizations, environmental changes are often ambiguous, requiring interpretation of what these changes mean (Pfeffer & Salancik, 1978; Chattopadhyay, Glick, & Huber, 2001). There is a need for trust in the interpretation of decisions made, impacting and impacted-on events, and processes that allow for sense making opportunities (Weick, 1995). The extent or levels of ambiguity are strongly dependent on the efficiency of the channels through which interpretations are made and transmitted (March & Olsen, 1975).

RM is the binding element between the two trends in two ways as it ultimately relates to trust in meeting demands and the expectations shaping the demands (Padró, Winwood, & Hawke, 2015). Regulators thus have to consider what to highlight, be it internal control systems which value technical properties enabling efficiency or have a preference for substantive improvement (Power, 2007). "[The] principles of regulatory necessity, risk and proportionality when applied in line with the Government's intention, support a high degree of autonomy which supports the aspiration from the sector and government for light touch regulation across the sector" (Dow & Braithwaite, 2013, p.2). As one of the questions in the 2013-2014 MBQNA (Baldrige Performance Excellence Program [BPEP], 2013) for Education criterion 1.2(b)(1) for *governance and social responsibility* regarding l*egal behavior, regulatory behavior, and accreditation* asks, "What are your key processes, measures, and goals for addressing risks associated with your educational programs and services and your operations?"

First of all, as the MBQNA criterion implies, RM becomes a policy conduit tying policy steering to definitions and performance parameters of quality. Quality practices have been seen to exhibit corporatist rather than pluralist tactics (active state intervention in the recognition of groups exercising a monopoly of interests representing a sector's needs and demands – Vandenberg & Hundt, 2012; Padró, 1988), particularly as it has developed in HEQA practice – although not as thought of by Tapper and Salter (1998). RM embodies the current ideas of public management, making up part of the rules for 'good' state regulation based on neoliberal lines of thinking (Power, 2007). I agree with Boas and Gans-Morse (2009), that the literature does not provide one primary definition of neoliberalism, thus for the purposes of this discussion, neoliberalism should be considered from the perspective of a development model based on:

> … a comprehensive development strategy with economic, social, and political implications… [involving] a set of economic theories linking disparate policies together into a coherent recipe for growth or modernization; prescriptions for the proper role of key actors such as labor unions, private enterprise, and the state; and an explicitly political project to carry out these prescriptions and ensure that actors play

> by the rules of the game… [with] implementation of a neoliberal model [involving] a restructuring of state-society relations (p. 144).

What seems to be the case is that RM is a proxy for a change in the relationship between universities and their stakeholders where autonomy is linked to a responsible partnership with government demands for accountability and business interests in knowledge acquisition and workforce development to improve leverage in a global economy (cf. Wueest & Fossati, 2015). "In balancing quality issues with the financial investment and return, higher education providers must consider intellectual property ownership, choice of partners, division of responsibilities, academic and business risk assessments, and internal and external approval processes" (Altbach & Knight, 2007, p. 302). Pursuing risk allows universities to gain or maintain market leadership by looking at the return on investment accrued from pursuing or discontinuing identified (and at times heretofore implicit) strategies (BPEP, 2013).

Secondly, process-wise RM acts as a *sense making* mechanism that transforms threatening encounters into managerial practice and managerial facts to support these practices (Hutter & Power, 2005). There is a constructed nature to the manner in which risk is defined and treated because it is an attempt at identifying not only what is happening, but what may be happening (Adam & van Loon, 2005). Risk is routinized and rationalized to create a sense of certainty by systematically noticing, bracketing, labelling, making presumptions about risk, communicating these to inform decisions and manage actions (Weick, 1995; Weick, Sutcliffe, & Obstfeld, 2005). Sense making results in intraorganizational evolution in formulating what can be evaluated to be stable acts in the future based on identified goals or (Weick, Sutcliffe, & Obstfeld, 2005), as well as quality criteria or standards. Stability is defined by the paradox represented in the need to demonstrate a balance between agility and resiliency in managing ambiguity and change with the maintenance of performance quality in meeting stakeholder expectations. Stability reflects the capacity to replicate success while change is the response to different stimuli, external and/or internal, making the mechanisms for these the same from a performative perspective (Feldman, 2003). This view is akin to Pascale's (1999) view of bounded instability as the emphasis is on balancing the tensions within the organization's units to achieve results rather than focusing on equilibrium of interests that emphasize a unit's security at the potential expense of organizational sustainability.

RM acts as another element of organizational double-loop learning through increased capacity for effective action by localizing and contextualizing the pattern of potentialities impacting organizational choice, eventually embedding their potential effects into an organization's decisionmaking machina (Kaplan & Norton, 1996; Senge, 2006). The addendum of risk into quality frameworks allows the ability to "incorporate future oriented risk management methods with quality methods that largely address historical data to provide an expanded skill set and consequently greater value to organizations" (Toney, n.d., p. 8). RM provides an opportunity to reconfigure and emphasize five dimensions associated with organizational decision-making practice: time, harm, chance, reward, and judgment. The reconfiguration and emphasis provides legitimizes "heightened accountability demands for adverse outcomes that could not be met by traditional organisational mechanisms" (Huber & Rothstein, 2013, p. 653) by aligning with organizational understanding from a SWOT perspective (Taylor, 2012; Evans, 2012; Padró, Winwood, & Hawke, 2015) in spite of potential limitations arising from what may be a brainstorming exercise that highlights the restrospection element of institutional sensemaking (Weick, 1995; e.g., Leech, 2012).

Australia's Tertiary Education Quality Standards Agency (TEQSA)

Australia became the first country to formally embrace RM in its HEQA scheme. In replacing the previous HEQA scheme – the Australian Universities Quality Agency (AUQA) – because it was not seen to be sufficiently rigorous on the sector reaccreditation (Bradley, Noonan, Nugent, & Scales, 2008). The one element that was kept was its risk framework (cf. AUQA, 2009). According to the Bradley Report,

> Criteria and processes for accreditation rely too heavily on subjective judgments and do not sufficiently reflect the risks associated with different providers… A formal risk assessment model would be required to underpin such a process with potentially different levels of regulatory oversight applying, including limits on a university's self-accrediting authority if necessary (Bradley et al., 2008, pp. 119, 122).

By statute, "TEQSA regulates higher education using principles relating to regulatory necessity, risk and proportionality, and using a standards-based quality framework" (Tertiary Education Quality and Standards Agency Act of 2011, p. 5). According to the Act, three reasons for this approach are to protect and enhance Australia's reputation for quality higher education and training services, its international competitiveness in the sector, and excellence, diversity, and innovative practices deemed appropriate to encourage and promote the nation's social and economic needs for a highly educated and skilled population. The role risk plays is to ensure that HEIs provide quality scholarship, teaching and research, student experiences, financial status and capacity through compliance with threshold standards. "Regulatory risk enables TEQSA to identify and understand risk to quality higher education, at both a provider and sector level, and informs decisions about where to focus and prioritise TEQSA's regulatory activity in response… by supporting a consistent approach to assessing the nature and extent of risk exposure of an individual provider, and guides proportionate regulation."(TEQSA, 2012, p. 3). The risk framework, however, is not intended to be a risk management tool for HEIs; instead, it is about the HEIs risk profile relative to the Threshold Standards based on both quantitative and qualitative data/evidence (TEQSA, 2012). Adding a risk framework provides the opportunity to reduce reliance on what the Bradley Report considered incomplete and subjective judgments in favor of evidence-based decisionmaking (Bradley et al., 2008).

Section 15 of the TEQSA Act mandates the Agency to look at risk to monitor impact in terms of an HEI's history relating to [1] scholarship, teaching and research; [2] students' experiences; [3] financial status and capacity; and [4] compliance with the Threshold Standards, the TEQSA Act and other laws regulating higher education. Section 15 also mandates the Agency to look at matters relating to the risk of the entity not complying with the Threshold Standards, the TEQSA Act or subsequent future changes regarding an HEI's [5] internal quality assurance mechanisms and financial status and capacity. The initial iteration of TEQSA's risk framework from 2012 was based on 3 overarching consequence areas: risk to students, risk of provider collapse, and risk to sector reputation for quality. Within these there were 8 risk categories aligned with the Threshold Standards: provider standing, financial viability and safeguards, corporate and academic governance, primacy of academic quality and integrity, management and human resources, responsibilities to students, physical and electronic resources and infrastructure, and other. These were based on thresholds identified through a traffic light system (with threshold formula). This system was based on 46 indicators seeking to pinpoint specific risks.

One major worry over TEQSA has been that it will focus on regulation at the expense of QA (Massaro, 2013). Concerns from the sector regarding burdensome regulation led to amending the Act, changes in TEQSA as an agency, and a refinement of the risk framework. The apprehensions come from challenges implementing the TEQSA legislation as well as its regulatory approach (Dow & Braithwaite, 2013). Version 2.0, the Risk Assessment Framework (RAF – 2014) simplified the approach to risk identification. This new version still maintained a focus on protecting students' interests and the sector's reputation by consistently and systematically monitoring key aspects of HEI operations (TEQSA, 2014). What was new was the recognition "that innovation often involves a degree of risk taking and does not consider risk as necessarily negative or that all risk must be controlled or eliminated.. [allowing] for expert judgement and embeds providers' history, context and own risk management within the risk assessment process" (p. 2).

Under the current RAF, there are two overarching areas: risk to students and risk to financial position. The third area, risk to sector reputation, is now embedded within risk to students by the focus on academic staff profiles, which is consistent with the view within program-level accreditation and USA-style accreditation practice concerning themselves with the appropriateness of the academic staff to teach the courses they do. The outlook is based on qualitative judgments in the analysis of risk indicators and how these are managed. Rather than 8 risk categories, Version 2.0 has 4 key risk areas: academic staff profile as discussed; regulatory history and institutional standing; student load, experience, and outcomes; and financial viability and sustainability. These are evidenced through 12 risk indicators plus an 'other'. "Considered together, these areas provide coverage across key aspects of providers' operations and all contribute to a view of potential risks to academic standards" (p. 5). The assessment of the risk indicators is performed holistically based on reference material, statistical analysis of the sector, TEQSA's experience from doing these analyses in previous risk cycles, and the nature (approach to and context) of the indicators. The 12 indicators are [1] cohorts completed, [2] student load, [3] attrition rate, [4] progress rates, [5] completions, [6] student satisfaction, [7] graduate destinations, [8] senior academic leaders, [9] student-to-staff ratio (SSR), [10] academic staff on casual work contracts, [11] financial viability, and [12] financial sustainability. The RAF again provides their formula to determine thresholds.

Adopting (adapting?) an RM framework

TEQSA's RM focus is regulatory and at the overall institutional rather than unit level. In the UK, HEFCE's approach until recently has been to concentrate implementing RM within HEIs (Huber, 2011). This is probably due to TEQSA embracing the BS 31100[1] standard's concept of proportionality (activities proportionate to the level of risk faced by the organization), but not the standard's concept of embedding, which HEFCE has pursued. New Zealand has a two agency approach to endorsing RM like the UK. In the USA, activity is at the organizational level, although adoption of RM practices has been voluntary, slow, and not in-depth (Association of Governing Boards, 2009) as similarly noted in Canada (Marsh Canada LTD, 2012). While MBQNA has included RM within its quality framework, the same cannot be said for institutional accreditation in the USA as SOX, especially Sections 302 and 404, focuses on corporate board composition and fiscal management controls. At the systems level HEQA agencies (as regulators) develop a comprehensive and uniform risk management template while HEI RM processes are expected to reflect the specific

[1] BS 31100 is a standard originally published in 2008 and updated in 2011 aligned with ISO 31000 providing principles organizations can use to form an RM scheme.

environment and institutional organisational skills which determine how it is structured and enacted concerning external, internal, and strategic risks and their impact (Huber, 2011; Arena, Arnaboldi, & Azzone, 2010).

At its most basic, RM is a system that links business strategy and objective-setting, controllability (control processes), accountability (assurance), and decision making (Arena, Arnaboldi, & Azzone, 2010; Gryna, 1999). An initial consideration is whether espousal is a sector level initiative, an institutional proposal, or both. Adoption, regardless of whether it is sector-based or HEI based is based on what RM is intended to do. Just like other areas of business, there is an increased recognition of the need to have fit-for-purpose risk systems. Recent surveys show an increased recognition that RM must fit purpose and RM activity ownership is a critical starting point as day-to-day operationalization is where the challenge lies (e.g., EYGM Limited & Munich Re, 2015). Taking a cue from Pergler's (2012) four stages of maturity, what is RM's purpose? Is it for transparency, systemic risk reduction, risk-return management, or risk as a competitive advantage (e.g., reputation)? The last point is an important one as it is a major determinant in which one framework is adopted based on treating the different forms of risk. Spikin's (2013) selection of risk classifications is useful as these various forms highlight the different sources and treatment of these risks: financial and non-financial, dynamic and static, systematic and diversified, pure and speculative, fundamental and particular, core and non-core, operational and strategic. The selection process for QAHE and HEIs is going to be framed by the extent to which risk is treated operationally (day-to-day and project-based) as well as strategic (larger-scale issues and thinking) and whether the thinking toward risk is going to be pure (loss-based only) or speculative (chance of gain or loss), as will be seen below. Particularly challenging is the perception of risk as being dynamic or static as this view tests the ability to identify and predict as well as test the level of understanding of what risk means at least at the organizational level (thus making the difference as to making RM meaningful rather than ritualistic, leading to deep rather than surface level organizational learning and decisionmaking applicability).

Based on previous work by Kaplan and Norton (2004) and Kaplan (2009), Kaplan and Mikes (2012) have proposed three qualitatively distinct categories of risk: preventable (avoidable internal risks), strategic (reducing the possibility that risk can materialize), and external (outside an organization's control). The literature suggests different risk types depending on industry and application. Figure 1 below is an attempt at identifying from the literature and placing different risk types within Kaplan and Mikes' categories within the higher education sector. Most of TEQSA's risk types fall under preventable risk because of their operational nature, the majority falling under compliance (internal accreditation processes), operational (day-to-day administration), and technological (technology enhanced learning and its delivery platforms) risks – these are not included in Figure 1 as it only identifies macro-level risks. Outcomes and culture are separated from operations in recognition of the risks that purpose, role (and institutional type), shared governance, and definition and enactment of unit level outcomes pose to operational contexts. Modeling (bias) and risk outside the box (ROB) are included because of the concern of self-fulfilling prophesies resulting outside organizational norms the need to recognize that there are unknown unknowns (not knowing where to look, what to look for, or exceptional circumstances/extreme occurrences falling outside expected outcomes or 'black swans' – Taylor, 2012). The end-game is to manage these different risks "that emerge from the routine, interlinked problems facing universities in delivering academic research and teaching, without comprising, for example, financial security, reputation and ethical conduct" (Huber & Rothstein, 2013, p. 657).

Preventable Risks	Strategic Risks	External Risks
Accountability	Financial	Political
Compliance	Human capital	Regulatory
Context	Information	Social
Cultural	Managerial	
Infrastructure	Modeling (bias)	
Insurance	Reputational	
Safety/Security	Risk outside the box	
Legal	(ROB)/New	
Operational	Supply	
Outcomes identification & results		
Technological		
Other		

Figure 1. Suggested risk type placement under the Kaplan & Mikes (2012) categories.

RM is often dealt with from a compliance perspective to align value and controlling staff behaviors, serving as a proxy for an integrated system aimed at generating discussion and debate (Kaplan & Mikes, 2012). The 2013 RIMS ERM survey indicates that board directives and regulatory requirements are two of the three major motivators for ERM implementation and that the influence of grass root efforts as drivers seems to be diminishing (Bradford & Fox, 2013). Consequently, imposing RM from a regulatory compliance purpose seems to generate the question of how deep into the HEIs should RM go and how it should look like, chiefly because of the need to focus more on resiliency than strict adherence to regulations. The question here is whether the sector and individual HEIs are comfortable with an audit-based, bottom-up tick-off the boxes approach rather than one of shoring up internal accountability practices as well. One concern, however, is if RM acts as a force for organisational conservatism rather than challenge and enhance organizational practice (Huber & Rothstein, 2013). A second concern is the capacity, experience, and training of staff assessing risks at the HEQA and HEI levels, but especially at the HEQA level performing institutional audit reviews (e.g., United States Government Accountability Office, 2011).

Sector level considerations

Recommendation or imposition of RM can be sectoral (by HEQA entities) or imposed by government agencies responsible for different parts of regulatory compliance or through policy steering considerations through legislation as part of the auditing and regulatory technology of government (Padró, 2014). The regulatory environment, derived from the policy steering agendae buttressing any HEQA, determines the approach to audits or organizational checks and which organisational 'truths' count as 'risk' (Stufflebeam & Coryn, 2014; Percy & Beaumont, 2008). Beyond jurisdictional issues, purpose and scope can suggest more than regulatory compliance. TEQSA (2012) defines *regulatory risk management* as "actual or potential risk events (regarding a provider's operations and performance) which indicate that the provider may not meet the Threshold Standards (either currently or in the future)" (p. 34). If policing is required because of trust issues based on abuses and wrongdoing and calls for reform, then top-down RM monitoring limiting HEI autonomy imposes additional requirements. For example, the HEQA scheme may have to be reconfigured to employ aggressive auditing programs to assure compliance with control

standards and/or establish in conjunction with the HEIs internal control (IC) standards to include procedures for separation of duties and access of funds (State of New Jersey's Commission of Investigation [SCI], 2007). If this last is to be the case, care has to be given to ensure that the audit process does not give too much credence to retrospective, historical data, something that is an inherent challenge given the timelines associated with formal auditing procedures.

HEI level considerations

RM adoption by HEIs seems to be based on whether it is imposed by the HEQA and thus treated as a reporting mechanism or internal interest is there to bolster their entrepreneurial, administrative, and engineering processes (Padró, 1988; Miles & Snow, 1978). Resurrecting the Miles and Snow breakdown of organizational structures and processes is useful in contextualizing RM for two reasons: it fits RM within the strategic and administrative processes and the distinction highlights the operational aspects of RM and the role IC plays throughout the HEI organizational structure. The distinction places the question about emphasis for use in the limelight: is it financial compliance or performance management? Less visible, but nonetheless, present are motivators such as a preference for risk aversion or maintaining reputational stability at all costs. Emphasis is important because it helps decide which RM framework to adopt. HEIs adopting RM have seen tangible macro-benefits deriving from consistent and systematic identification, assessment, and seized opportunities in ways that were not necessarily possible before (HEFCE, 2005). HEFCE looks at RM "as a matter of high-level governance and accountability, not a specialist activity carried out by a small unit some distance removed from everyday operational routines" (Hommel & King, 2013, p. 3). However, no one role model or set of metrics has emerged as the top-down model is too narrow and practices are adapted rather than copied to meet contextual preferences and what fits one organization does not another (Huber, 2011; American Productivity and Quality Center, 2007).

Traditional RM is based on the identify-assess-treat (IAT) model in which risk is treated as a by-product of actions and thus performed post-fact (Jablonowski, 2007). One common practice in RM is the use of a risk register. Often, these focus on operational, financial, objective (outcome), reputation, and other risks as exemplified by register made available by Logframer (http://www.logframer.eu/content/exporting-risk-register-new-ms-excel-workbook) or through the University of California (http://ucop.edu/enterprise-risk-management/tools-templates/risk-assessment-toolbox-content/higher-education-risk-assessment-tool.html). The register provides a *probability x impact* method to rationalize potential risks and improve the HEIs' understanding of these to make more rational, efficient and legitimate decisions (Huber & Rothstein, 2013). It does so through identifying potential risks by types, the potential impact from these risks, the likelihood of risk occurring, how to manage and mitigate risk, types of controls required and their effectiveness, what monitoring and reporting procedures are needed, and who is responsible (ownership). Implementing a risk register brings forth the need for a series of institutional decisions: [1] for external reporting purposes, suggesting an external monitoring process that can be separate from internal feedback loops for assurance or process (quality) control/management[2] or [2] embedding RM within the existing feedback loops. The former approach allows for a separate audit process with its own timelines or one that is aligned with existing internal QA

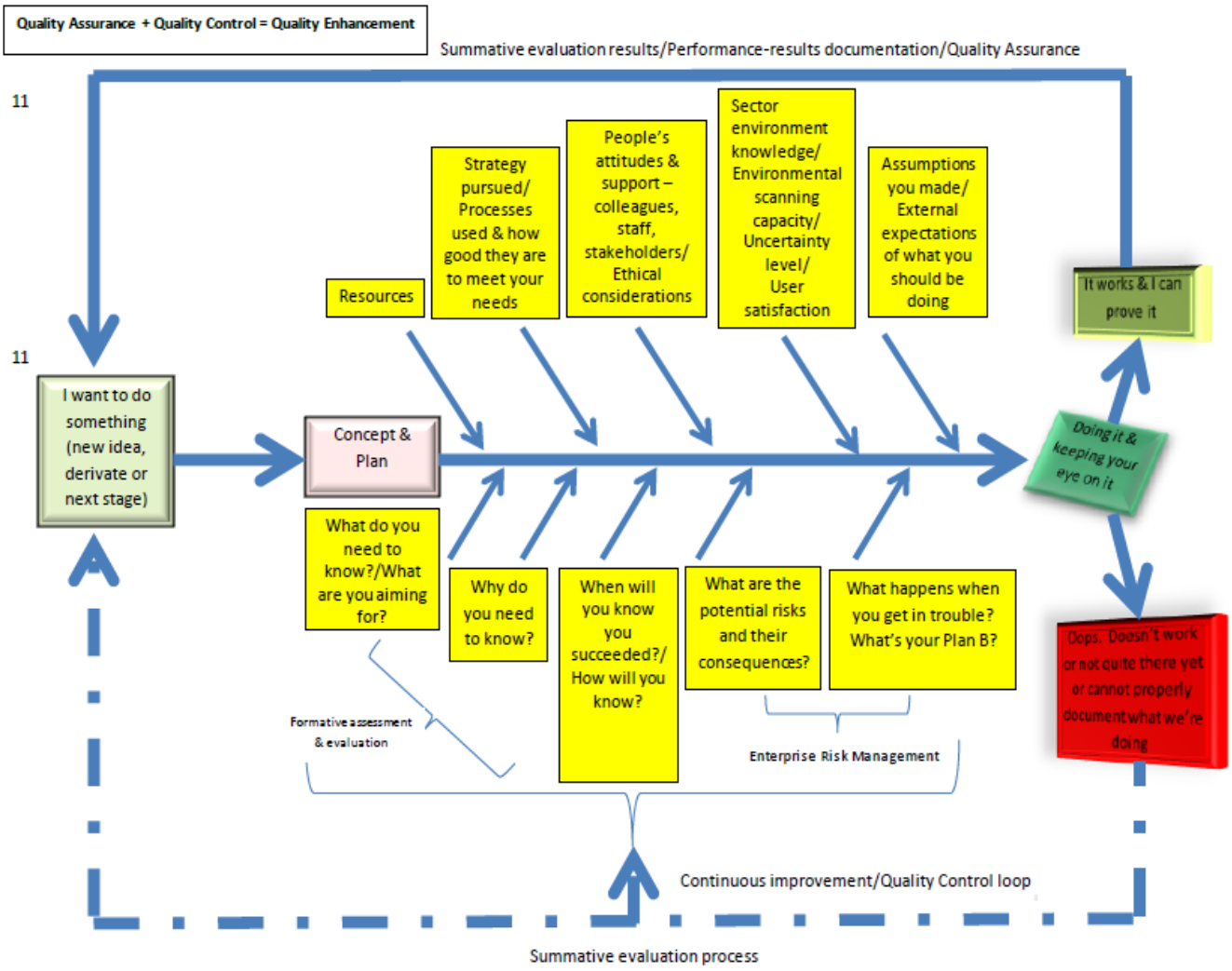
[2] Juran and Godfrey's (1999)'s definition of quality control (QC) is useful: a managerial process for conducting operations to provide stability (prevent adverse change) by evaluating actual performance, comparing performance to goals, and taking action on the difference.

auditing activities only.[3] The latter, supporting Arena, Arnaboldi, and Azzone's (2010) point of RM's fluidity, integrates RM into existing ongoing (formative) and/or retrospective (summative) evaluative frameworks where judgments of the performance of at least academic and support programs are based on criteria or standards of antecedents, transactions, and outcomes (Stake, 1967). Quality frameworks and evaluation frameworks can have different data requirements and techniques for analysis and/or review. Selection of quality-evaluation models requires an understanding of these models, measurements, and relationships to obtain objective assessments (Tian, 2004) and judgments. One prevalent model within the educational arena that fits Tian's view of quality-evaluation because of its adaptability and focus on objectivity and improvement orientation is Stufflebeam's Content, Input, Process, Product (CIPP) framework that is used for reviewing/auditing goals, plans, actions, and outcomes (Stufflebeam & Cronyn, 2014).

Figure 2 breaks down HEI QA, QC, and evaluation processes and illustrates where RM can fit into these processes. The various elements within these processes also suggest how a SWOT process can be involved as well (Padró, Winwood, & Hawke, 2015).[4] This is consistent with BPEP's (2013) view that the level of intelligent risk differs by pace and level of threats and opportunities faced by HEIs. It is also acknowledged as good practice by HEFCE (2005, p. 28) and the Institute of Management Accountants (Shenkir &Walker, 2007). Figure 3 demonstrates how a SWOT process does integrate into existing quality-evaluation frameworks using various aspects of CIPP often applied to campus activities. The integration of these approaches permits RM to be embedded it into the daily campus activities by individuals and teams in a manner that embraces existing cultural values rather than making it feel as 'bolted-on" and decreasing its chances to achieve desired results (HEFCE, 2005).

[3] Different surveys show that when internal and external auditing processes are performed by the same agents without safeguards implicit in staff separation, independence and reliability perceptions are significantly reduced (Hill & Booker, 2007).

[4] The literature also suggests the use of brainstorming and/or Monte Carlo analysis as part of the risk analysis. SWOT is preferred because it is a more structured approach to brainstorming and allows decisions to be identified and plugged in as an extension of a risk registry that can be part of an existing internal decisionmaking framework. The Monte Carlo method is based on providing a statistical probability of outcome by assessing the range of considered variables, determining the probability distribution of each variable, and repeating the process as many times as needed to get the average impact of the risks over the course of the entire project (PMI, 2013) or strategy.



Source: Padró, 2014, p. 8.

Figure 2. HEI QA and QC assessment and evaluation activities

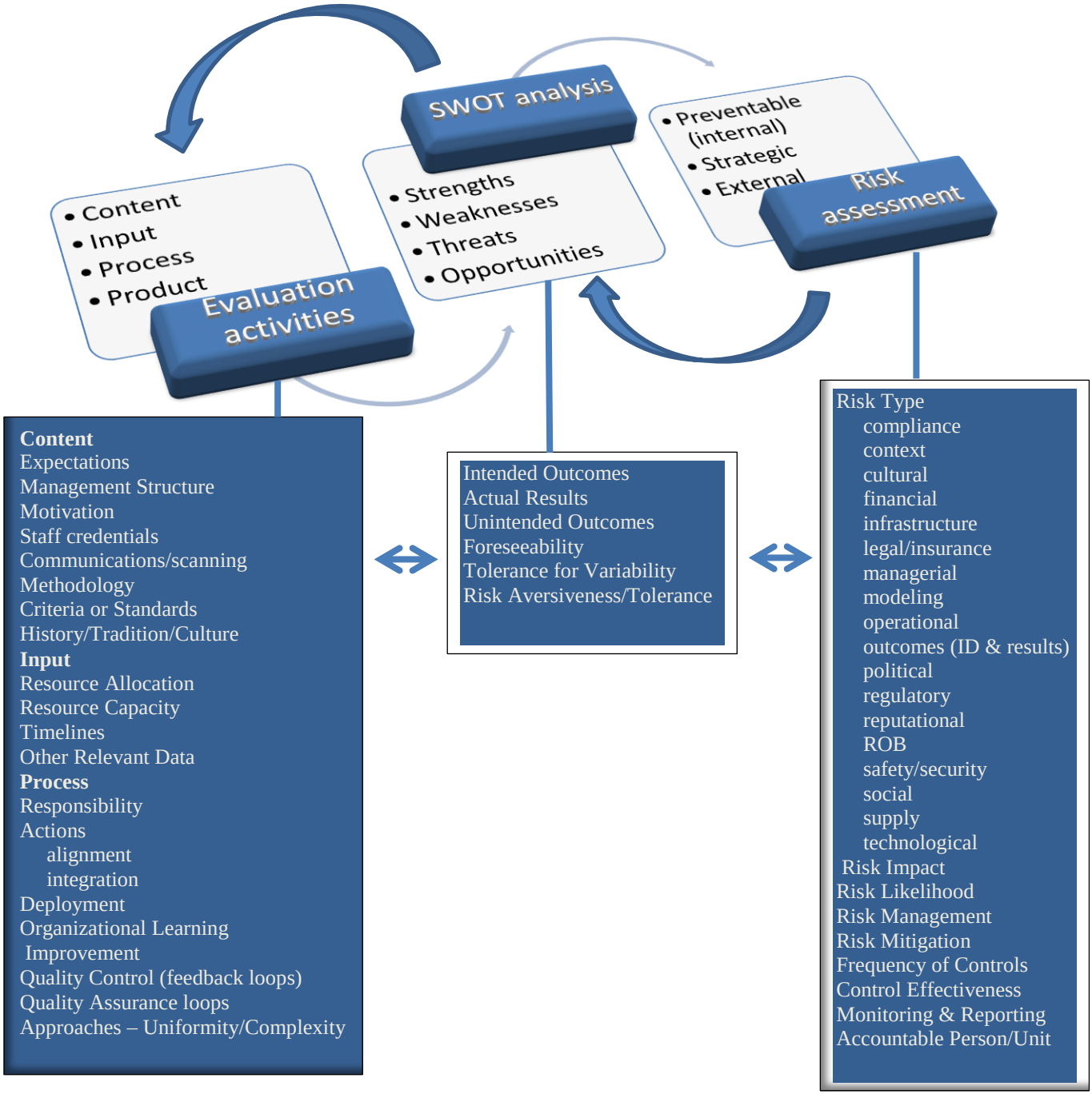


Figure 3. Linkage between ongoing HEI evaluation activities, risk assessment, and SWOT analysis.

Defining risk – Sectoral preference so far

So far missing in the narrative is a definition of risk as such. The reason for this is that different frameworks provide a different approach to risk that becomes a guide for organizations when selecting which one approach to adopt. Therefore, another question that should be asked is about the approach to risk a national higher education sector wants to pursue. The interdisciplinary definition of risk is consistent in the view that it is a function of likelihood and impact (Padró, 2014). The difference in defining risk relates to the extent to which risk can be seen and treated as an opportunity rather than only a liability or threat *vis a vis* consequences. As is seen later in this paper, this is one of the major differences between the COSO framework and the ISO 31000 standard.

A key figure in the risk literature, Ulrich Beck (2009) views risk as partly defining a social relationship between at least two people: a decisionmaker who assumes the risk based on actions and others who receive the consequences of these actions. "Risks pose in principle the question (which combines defence and devaluation) of what "side effects" a risk has for others and who these others are and to what extent they are involved in the decision or not" (pp. 3-4). However, the prevailing view in the practice of RM is based on F.H. Knight (1921), who argued for the linkage between profit, quantifiable risk, uncertainty, and inherent ambiguity.[5] As he pointed out, there is fundamental distinction between taking a known versus an unknown risk and how context and environment influence the impact and value (determinate and indeterminate) of risk to an organization. He also talked about the difficulty in ascertaining the value of risk. Knight, though, only looks at risk from the perspective of uncertainty rather than the more modern view of defining risk in the terms of uncertainty **and** exposure (Holton, 2004). Holton nonetheless concludes that this definition of risk does not work operationally because what can be measured is the perception of uncertainty and exposure.

I agree with Rao and Goldsby (2009) that there is more literature on managing risks than there is on research associated with identifying risks and on the definitional issues surrounding what risk is and its treatment. This is interesting in that Beck (1992) notes the importance of looking at risk in terms of relation of definitions. Risk cannot be transformed into security as it is a question of attribution – and in today's society this means a societal problem generating responsibility (Holmström, 2007). Different professional organizations have generated their own definition of risk and supporting RM framework. So too have some of the social sciences disciplines like anthropology, economics, political science, psychology, and sociology (cf. Luhmann, 1993). Most of the professional associations focusing on risk come from the fields of accounting, banking, and insurance while government agencies provide standards specific to other fields such as technology. Figure 4 provides an example of how some of the key players define risk or examples of how derivative definitions within their model shape the approach taken to risk. The preponderance of the definitions in Figure 4 reflects the potential for upside as well as downside impact of risk on an organization. It is interesting to note that the project manager associations (FERMA, PMBOK) take on this view from early on while a more conservative view is noted from the banking (Basel II) and actuarial organizations (Solvency II), although the field of accountancy (IIA) tends to couch the definition more neutrally, seeming to focus more toward the negative rather than positive potentialities from identifying and treating risk. NIST's definition also slants toward only ascertaining the negative potential of risk as it seems to focus more on the safety and security components of technological developments from a compliance/preventive perspective.

[5] The literature from sociology on risk challenges the technical definitions of risk as seen in current practice (Zinn, 2010), but the inclusion of this literature as well as from the other social sciences helps frame and broaden the discussion of applicability of RM within QAHE.

Professional organizations	
Professional organization	**Definition of risk**
Basel II (Basel Committee on Banking Supervision, 2002)	Operational risk: The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.
Federation of European Risk Management Associations (FERMA, 2002)	An uncertain future outcome that can either improve or worsen position – superseded by ISO 31000:2009
Solvency II (Groupe Consultatif Actuariel Européen, 2007).	Compliance risk: legal or regulatory sanctions resulting in a financial loss, or loss of reputation as a result of an insurer's failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct. Operational risk: change in value caused by the fact that actual losses, incurred for inadequate or failed internal processes, people and systems, or from external events.
Risk and Insurance Management Society (RIMS, 2012)	An uncertain future outcome that can either improve or worsen position
Institute of Internal Auditors [IIA] (2013)	The possibility of an event occurring that will have an impact on the achievement of objectives, measured in terms of impact and likelihood.
Project Management Body of Knowledge [PMBOK] (Project Management Institute [PMI], 2013)	An uncertain event or condition, that, if it occurs, has a positive or negative effect on one or more project objectives.
Government agency or Social group	
Government agency or social group	**Definition of risk**
National Institute of Standards and Technology (NIST , 2010)	Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Open Compliance and Ethics Group [OCEG] (Mitchell, Switzer, & Mefford, 2015)	Risk identification: Identify forces that may cause desirable (opportunity) or undesirable (threat) effects on the achievement of objectives, as well as those that may compel the organization to conduct itself in a particular way (requirement).

Figure 4. Definitions of risk or derivate definitions of risks suggesting an approach to defining risk from professional associations/organizations, government or social organizations.

Beck (2009) opines that risk is not merely a side effect and that, paradoxically, attempts at managing the complexity of risk falls back on abstractions and models that generate new uncertainties. Certainty in what is happening increases risk aversiveness as well as the desirability of gains (Kahneman & Tversky, 1979). Framing of the acts impacts perception and decisions (Tversky & Kahneman, 1981) which set how institutional or sectoral dilemmas in risk are identified and treated as it shapes and/or directly or indirectly defines bias (Jablonowski, 2007). Within a QA scheme, limiting scope to avoidance minimizes the capacity for generating opportunity from a non-defensive posture while increasing a new risk, that of inaction or procrastination. Qualitatively, both opportunity and risk encompass uncertainty. Opportunity can be defined as "an uncertain event or set of conditions that … would benefit the project or business' (Hillson, 2004, p. 18). Opportunity equates improvement as a form of value creation for the organization by encouraging the exploration of new responsive initiatives from dealing with unpredictable environments (Andersen, Garvey, & Roggi, 2014). As Hillson (2004) points out, the definition of opportunity is similar to the definitions of risk such as those included in Figure 4, which is why he believes a definition of risk based on opportunity and risk makes sense.

So far, the majority of higher education sectors utilizing RM as part of their HEQA scheme have taken the side of risk as a threat and an opportunity. HEFCE (2001) defines risk as "the threat or possibility that an action or event will adversely or beneficially affect an organisation's ability to achieve its objectives" (p. 4), with risk possible at the corporate or strategic, faculty, departmental, and personal levels. Couple this definition with TEQSA's (2012) previously provided definition of regulatory risk and BPEP's (2013) definition of intelligent risk as "[opportunities] for which the potential gain outweighs the potential harm or loss to your organization's sustainability if you do not explore them" (p. 47). Together these provide a yardstick to use when considering which approach to RM is appropriate based on the perspective found in the ISO 31000 standard.

A different approach is pursued in the USA as they have not pursued a regulatory risk approach as Australia has and the UK is about to impose. RM adoption has been voluntary and at the HEI level through espousal by NACUBO (2003), although a number of state QAHE schemes have adopted many aspects of Sections 302 and 404 of the Sarbanes-Oxley Act of 2002 (SOX) that applies mainly to publically traded organizations (Padró, 2010). Section 404 in particular lays out IC expectations. Consequently, there is no one prescribed approach to scope and process of how assessments and evaluations are made. The legislation does not define risk as such, but in its demand for risk assessment, it is closely aligned to the COSO's ERM framework and its definition of IC (cf. Institute of Internal Auditors, 2008; Protiviti, 2013). SOX's language as its top down emphasis of control and responsibility fits well with COSO's 2004 definition of risk based on its 1992 model:

> … a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

COSO's 2013 definition is less expansive as seen below, but the RM and IC approaches still resemble the earlier definition as it maintains a preference for board level control is more preventive than opportunistic.

COSO and ISO 31000 frameworks

Various organizations have attempted to define an RM framework from the 1980s onward, with two rising to prominence, the COSO framework and ISO 31000 (Power, 2007; Charette, 2010). The differences in approaches and definitions represent the interdisciplinary interests, issues, and treatments of risk. COSO's framework has primarily been applied to organizations in the USA as well as internationally while ISO 31000 represents a more international practice with origins in the Australia and New Zealand AS/NZS 4360: 1999 Standard (Australian/New Zealand Standards, 2009).

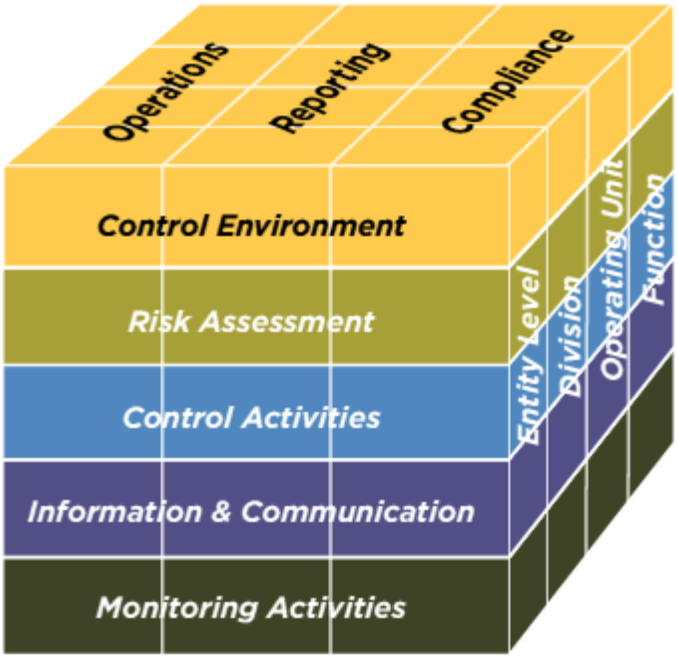
COSO

COSO's developmental history shows conceptual similarities with ISO 9000 (Moeller, 2014; Power, 2007) that make the parallel or embedded interaction between RM and quality management systems possible. Its initial focus was to study the causal relationships leading to fraudulent financial reporting (Protivity, 2013). In doing so, it created new product opportunities for the accounting profession (Power, 2007). COSO stresses auditing over risk management, making it attractive for regulatory purposes and less so for internal quality management purposes. Part of the reason for this is the concern over the blurring between external and internal auditing and the negative legal impact outsourcing of auditing had on companies that performed other services for the contracting organization (Moeller, 2014).

COSO's IC framework, originally created in 1992, was revised in 2013. It was designed to be complementary to its more expansive ERM framework.[6] COSO's ERM Framework concentrates on acceptance, avoidance, reduction, and sharing of risk whereas COSO's IC Framework's main interest is risk reduction. The definition of IC did not change.[7] Neither did its five components: control environment, risk assessment, control activities, information and communication, and monitoring activities. The approach remains a multi-faceted, multi-level concept, with objectives that link all organizational components with the three dimensions of the framework (operations, reporting, compliance – Figure 5). The update was meant to make COSO more robust, with the major change beings that the principles supporting the five components of IC were codified into 17 principles (Figure 6). These principles are supported by 85 points of focus intended to provide guidance in designing, implementing, and controlling processes and assessing if these are present and functioning (Moeller, 2014). Generally, the points of focus, when applicable, are intended to [1] set the tone at the top, [2] establish standards of conduct, [3] evaluation of adherence to standards of conduct, and [4] addressing deviation in a timely manner. Protivity (2013) describes the other changes made as [1] clarifying the role of objective-setting in IC, [2] reflecting the increased relevance of technology, [3] incorporating an enhanced discussion of governance concepts, [4] expanding the reporting category of objectives, [5] enhancing consideration of anti-fraud expectations, and [6] increasing the focus on non-financial reporting objectives and how conformance requirements such as ISO 9000 fit within the framework (McNally, 2012).

[6] For this paper, the term RM is used so as not to focus on organizational or enterprise risk management (ERM) promoted by COSO or regulatory risk management (RRM) as identified by TEQSA. ERM is seen as a strategic model that is different from traditional or previous risk management thinking that was more silo-based (Gatzert & Martin, 2015).

[7] Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.



source: Protiviti, 2013, p. 2

Figure 5. COSO 2013 IC Framework

Control environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

source: Adapted from Moeller, 2014, p. 38.

Figure 6. COSO 2013 17 internal control principles

ISO 31000

Written by risk managers and international standards experts (Gjerdrum & Peter, 2011), ISO 31000:2009 superseded AS/NZS 4360:2004. Working definitions of key concepts and terms come from ISO document Guide 73:2009. "While all organizations manage risk to some degree, this Standard establishes a number of principles that need to be satisfied before risk

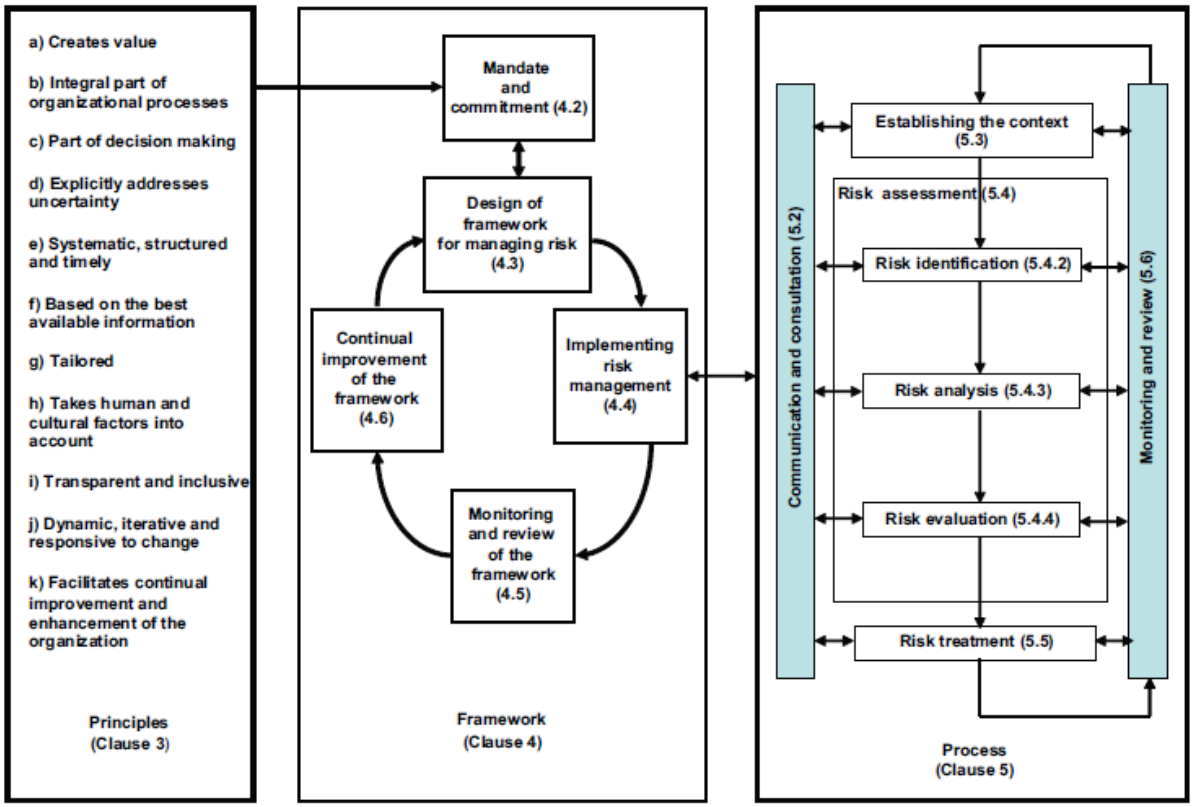
management will be effective" (Australian/New Zealand Standards, 2009, p. iv). More importantly, ISO 31000 is not intended to promote RM uniformity for an industry or sector or across organizations. Its context is similar to Kaplan and Mikes' (2012) in that it recognizes and works from internal, external and strategic (process) perspectives. The Standard provides a generic guideline on how to embed RM in a manner consistent with HEFCE's (2005) view of good practice:

- responsive to the institution's objectives, organisation and environment;
- owned by management;
- built into the way business is conducted; and
- regularly and relevantly reported (p. 27).

Rather than upholding the interests of external and internal auditors plus the finance office to the extent COSO can, ISO 31000 is intended to meet the needs of diverse stakeholders such as [1] those accountable for achieving objectives (who need to ensure risk is effectively managed within the organization institution-wide, unit level, for a project or activity), [2] those responsible for developing risk management policy within the institution, [3] those who need to evaluate an organization effectiveness in managing risk, and [4] developers of standards, guides, procedures, and codes of practice who need to manage risk within the specific context of these documents. Unlike COSO, the Standard is not intended to be a compliance standard, even though ISO 31000 welcomes being adopted by any community, private, or public entity in any sector. "Organizations with existing risk management processes can use this Standard to critically review, align and improve their existing practices" (Australian/New Zealand Standards, 2009, p. v).

ISO 31000 is composed of three inter-related elements: principles for managing risk, the framework to enact the principles, and the RM process (Figure 7). *Principles* support a comprehensive and coordinated view of risk that applies to the entire organization and link the framework and processes to organizational strategic goals (Gjerdrum & Peter, 2011). The framework assists in managing risks effectively through the application of the RM process, ensuring information emanating from RM is adequately reported and used as a basis for decisions. "The component parts of the *framework* include establishing the mandate and commitment to risk management, designing the framework for managing risk (which includes understanding the organization's internal and external context, establishing a risk management policy, integration of risk management into organizational processes, internal and external communication and reporting and allocation of appropriate resources), implementing the risk management process (details follow), monitoring and review of the process and continual improvement of the framework" (p. 9). The RM process steps are establishing the context, risk assessment (identification, analysis, and evaluation), and risk treatment. According to Gjerdrum and Peter (2011):

> In the ISO model, they are central to the process of managing both individual and portfolios of risks. A significant difference from the traditional process is that the ISO model includes the elements of 'establishing the context' and continuous 'communication and consultation'… Then, in addition to the core steps of the process, the ISO Standard identifies two key functions that should happen continually throughout the risk management process: 1) Communication & Consultation, which needs to be built into the process and involve both internal and external stakeholders, and 2) Monitoring & Review, which occurs continually during the process. (p. 10).



source: AS/NZ ISO 31000: 2009, p. vi.

Figure 7. Relationships between the risk management principles, framework, and process

Selecting an RM framework

Selecting which framework is in itself a major strategic decision as is its operationalization, assuming that it will be done systematically rather than as-needed as it takes away the anticipatory aspect of RM (Tufano, 2011). According to BPEP (2013), "[choosing] which strategic opportunities to pursue involves considering relative risk, financial and otherwise, and then making intelligent choices ("intelligent risks")" (p. 11). The development of regulatory risk reflects a policy steering preference for preventive solutions. This establishes mission risk in addition to all the other forms already discussed and one reason regulators have been guiding RM practices by suggesting techniques and determining what risks are included into RM frameworks within organizations (Power, 2007; Mikes, 2005). However, care has to be taken to ensure that the implemented RM scheme represents organizational realism because of the noted differences in outcomes between, for example, cross-functional groups and financially oriented groups (Martin & Power, 2007; Blaskovich & Taylor, 2011). For a sector RM with a regulatory focus, the United Nations Economic Commission for Europe (2012) suggests the following activities:

- setting the regulatory objectives;
- providing traceability in supply chains and management of assets;
- risk identification: identifying the risks to those assets (including intangible ones, like public health);
- risk analysis and evaluation: understanding the most important risks;

- choosing risk treatment strategies;
- implementing risk treatment strategies;
- crisis management (including developing a plan to deal with disruption-related risk); and
- monitoring, reviewing and improving the risk management process (p. 85).

Context for setting the boundaries for the RM scheme is shaped by the sector agency's external and internal environment; the risk profile, risk appetite, risk tolerance levels, and risk matrix and responsibilities the above activities generate; and contingency plans for business continuity (Queensland Government, 2011). Moreover, as the banking sector found out after the subprime crisis, consideration should also be given to resilience (O'Shea & Krischanitz, 2013).

At HEIs, the framework selected has to consider their unique culture and how the governance and management structures work together. Issues of non-quantifiable risks and resource allocation are contestable as these points fall into the fluid nature of organizational politics (Mikes, 2005). A key point here is whether to integrate what may be a *de facto* silo approach to RM because of its disaggregate locations and uses – which is seen to be the least effective – or establish integrative processes that allow for clear lines of communication from central administration to the various channels of shared governance where participation by academic staff in particular is predominant. This last point is inversely proportionate to the extent the university culture is corporatized *vis a vis* faculty controlled.

Consistent with this paper's narrative, Mikes and Kaplan (2015) echo other beliefs and findings throughout the literature regarding the composition of a set of RM components within an organization:

- a process for identifying, assessing, and prioritizing risk,
- linkages from risk management to other important control processes,
- frequency of risk meetings (based on treating risks as dynamic or static, distinguishing treatment of strategic and/or operational – day-to-day and project-based), and
- risk tools (grounded on a cultural predilection of quantitative enthusiasm or scepticism.

The second bullet point is particularly important to HEIs. Campus interactions have symbolic meanings. "What becomes tightly or loosely coupled in this symbolic system is related to a mixture of collegial interactions, bureaucratic structures, ongoing coalitions, chance, and cognitive processes by which people make inferences and judgments under conditions of uncertainty" (Birnbaum, 1988, p. 160). As Birnbaum (2000) later pointed out, long-range planning schemes worked well under traditional approaches to managing HEIs – what he terms *Ur Management* – only when the driving assumption is that the future is going to look pretty much like the past and the focus was more on inputs than outputs. Putting together an RM framework necessitates a conscious rather than tacit consideration of avoiding what Birnbaum (1988) termed traits of an anarchical institution: *problematic goals* (a silo-based problem when different academic and non-academic units are involved in performing similar or overlapping functions), *unclear technologies* in achieving desired results (the risk tools that are put in place), and *fluid participation* (a not fully defined process for identifying, assessing, and prioritizing risk, the frequency, purpose, and types of interaction between key players and the governance structure in which it all happens). One potential occurrence under

these conditions is awareness of the possibility of solutions looking for problems to meet a particular agenda.

An example of how an HEI has engaged with RM, the University of Adelaide (n,d,) looks at risk as value enhancing and/or value protecting, undertaking activities that are adequate and appropriate in maximizing benefits and minimizing the negative or unanticipated effects from risks or opportunities presented in the achievement of organizational objectives. Per suggested practice, the University identifies key participants and their responsibilities. Its application of RM is for:

- systematizing evidence and improving assurance;
- enhancing and improving decisionmaking;
- formulating more convincing and better substantiated proposals;
- fostering more practical approaches to dealing with problems or issues;
- better manage activities where adverse events may arise;
- increased learning from previous mistakes;
- enhancing good governance, brand and reputation, communication, reliability, ability and confidence;
- reducing hasty, rash, or poorly considered decisions; and
- reducing uncertainty around objectives, inconsistency in decisionmaking, procrastination due to uncertainty, adverse events or negative consequences, unanticipated or unplanned events, embarrassment or discredit from poor outcomes (p. 7).

"Both COSO ERM and ISO 31000, because of their maturity, their holistic approach and their methodological consistency, can help organizations to realize the potential benefits connected with the application of a generic risk management standard" (DeLoach, 2012). Each has its limitations and detractors as well as benefits (hopefully, more than conceptual in nature. And for those looking for empirical studies or other evidence of their effectiveness, there is not much out there as of the time of this writing, particularly in higher education. What Mikes and Kaplan (2015) found so far is that some of normative literature on organizations verifies the influence of boards and executive teams in securing ERM adoption while other studies find the presence of an internal risk specialist as a driver or that firms carrying higher levels of risk distress are more likely to adopt ERM. Gatzert and Martin (2015) have also found that, in general, what there is of empirical evidence is in line with theoretical considerations although comparability is limited These findings are consistent with Mikes and Kaplan's (2015) observation that empirical findings of less–than-obvious contingency variables are mixed or contradictory, with stock-priced studies attributing value to ERM showing mixed results, suggesting that effectiveness has less to do with the framework in regards to the quality depth and impact than on people who set it up, coordinate and contribute to it, and that practices differ across firms, even within an industry.[8]

There is a fundamental difference between both models although overall, there are more similarities and differences reflecting who were behind the writing of these frameworks (Bugalla, Narvaez, & Kallman, 2012; Gjerdrum & Peter, 2011). The similarities between both are palpable in TEQSA as it definitely promotes the ISO 31000 approach, but its top-down regulatory approach is consistent with the COSO framework too. Where they differ is

[8] Both of these articles cite specific studies the reader may want to consider, with Gatzert and Martin's appendix providing a more comprehensive number of studies on the determinants of RM.

that ISO 31000 focuses more on implementation and managerial while COSO is accountancy based. COSO is complex and multilayered, which is why supporters and detractors discuss the difficulty organizations have had in implementing the 1992 versions – the verdict is still out on the 2013 changes. In contrast, ISO 31000 is seen as simpler to understand and implement. ISO 31000's strength may also be its weakness: its generic nature may require an HEI spend significant time and resources to implement (Charette, 2012). Both frameworks are guides that HEQAs and HEIs can use to pursue an RM scheme. Practitioners suggest the possibility of combining both to meet specific needs, but the trend seems to be using one or the other. A concern, or even a risk itself, is that without careful aforethought "[financial] control reporting becomes yet another risk management silo with its own vocabulary and methodology - a framework that is not consistent with all other ERM work done on every other facet of the organization's operations" (Leech, 2012, p. 18).

In an approach similar to Gjerdrum and Peter's (2011) article, Figure 8 takes on key definitions from both frameworks to highlight their approaches to key RM concepts. Not all definitions are the same ones presented in Gjerdrum and Peter's analysis as the focus here is on the specific approaches to the term risk itself to highlight the issues so far identified in this paper. Figure 8 uses terms often highlighted in the literature that are bridgeable between the two frameworks to demonstrate similarities and differences in approach and conception.

Similarities and differences are apparent when both frameworks define the same term. The differences in thinking become ostensible when the attempt is made to bridge the divergent concepts between COSO and ISO 31000. The biggest difference as can be seen is in the definition of *risk* itself – from probability of loss (COSO) to the effect of uncertainty on organizational objectives (ISO 31000). A discernible issue that should be noted is the capacity for COSO to recognize risk emanating from slow, gradual change given that its focus is on sudden, major impact change.

Figure 8 shows that the definitions of *risk appetite* between the two frameworks are similar, although ISO does prefer to identify type as well as amount based on organizational preferences. *Risk appetite* under both frameworks is a strategic driver of operational and strategic organizational decisions regarding their willingness to pursue, continue, or engage in activities to achieve identified outcomes – setting boundaries as it were. The slight difference reflects the lack of consensus on its meaning or practical application (Hillson & Murray-Webster, 2011).

COSO and ISO 31000 use a different vocabulary in dealing with the notion of magnitude of risk that organizations can/will accept. ISO 31000 refers to this as *level of risk*, stressing the consequence of events and the resulting impact on organizational objectives. COSO refers to this effect as *risk tolerance* (both of these have a dark orange background in Figure 8). Under COSO, *risk tolerance* is related to *risk appetite*, but with one major difference: "risk tolerance represents the application of risk appetite to specific objectives" (Rittenberg & Martens, 2012, p. 11). This is why Rittenberg and Martens also treat *risk tolerance* as determining flexibility while risk appetite is what sets the organization's limits.

ISO 31000 provides a definition for *risk evaluation*, but COSO does not. Instead, COSO talks about *risk response*. ISO focuses on the process of comparing results based on defined risk criteria whereas COSO looks at assessment based on likelihood and impact, costs and benefits, and aligning these to acceptable level of tolerance (the definitions of risk evaluation and risk response are in dark grey in Figure 8). Viewing the terms together, the terms are

looking at a value judgment of the actions rendered, suggesting similarity rather than dissimilarity. This point is strengthened when looking at how both frameworks define *risk assessment*. From a higher education perspective it is worth proceeding from the perspective of academic practice as there is a typical blurring of concepts that may be irksome to some academics. These various definitions refer to two different activities: assessment as the gathering (measurement) of information and the use of the information for improvement purposes (evaluation), with the distinction being blurred based on the purpose(s) behind the activities (Astin & Antonio, 2012). Additionally, COSO's *risk response* also can be linked to ISO's *risk treatment*, as this last is about what is done as a result of the assessment/evaluation. As a modification process, *risk treatment* decisions can be [1] avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk, [2] taking or increasing risk in order to pursue an opportunity, [3] removing the risk source, [4] changing the likelihood, [5] changing the consequences, [6] sharing the risk, [or] [7] retaining the risk (Hardy, 2010, p. 12). Purdy nonetheless finds that *risk treatment* as found in ISO 31000 clears confusion that exists from looking at implementing COSO's *risk response*, control activities, and monitoring:

> Risk treatment refers to the actions you take that lead to the creation of and improvement in controls, and controls are what you employ to modify risk. These controls then require monitoring and review by assurance processes. That's it" (Marks, 2011, February 21).

Part of the overall risk assessment process (Moeller, 2014), COSO's *inherent risk* is a measure of likelihood and impact of an identified risk or risk without controls. It becomes a reference point in the risk register (as a starting point), helping rate the probability that risk can occur. *Inherent risk* is linked to *residual risk* (red in Figure 8) as it helps determine if the level of risk remaining after its management or mitigation is acceptable to the institution at a future point in time (Protiviti, 2013). COSO looks as both of these as risk if nothing is done and what risk is left after doing something (Curtis & Carey, 2012). Purdy points out that *inherent risk* is not intuitive to practitioners because it represents an artificial and theoretical state without controls to justify tolerating the present level of risk (Marks, 2011, February 21). *Residual risk* is used by both frameworks. As Protivity (2013) points out, risk responses seldom eliminate risk and the idea is to seek practical solutions that hold risk to tolerable levels without unknowingly incurring another risk.

Although not linked in the literature, a case can be made that COSO's *inherent risk* can also be linked with ISO 31000 *risk source* (red in Figure 8 as well) because different activities do have their own level of risk. Business as usual (BAU) and ongoing projects tied to BAU are a potential risk source with an inherent risk capacity, and not just special projects extending, implementing, or improving existing activities.

Both frameworks define RM (Figure 8, light blue). COSO's definition is purposefully broad, emphasizing how control emanates from the top of the organization. The emphasis is on the top managing down, with bottom-up reporting. This tends to be contrary to the notions of university governance at HEIs that are not overly bureaucratic in nature or corporatized, especially shared governance, but the top-down preference is one typically noted in the QA and QAHE literature streams. A further read of the COSO framework implies that processes have to be firmly aligned and somewhat subordinated to fiscal reporting and demonstration of regulatory compliance as means to assuring quality (cf. Padró, 2010). This is not surprising because there seems to be similarities in approach to the Basel II, Solvency II, RIMS, and IIA

models (Figure 4) that come from the accounting and financial sectors. ISO 31000 shares many features found in the practice of project management (cf. PMBOK, 2013), as can be noted in the definitions of risk provided in Figure 4 above. The approach is more governance process based as indicated in ISO 31000's risk management framework (which is why it is also light blue in Figure 8). RM under ISO 31000 is intended to address a wide range of stakeholders responsible for ensuring risk is effectively managed (Gjerdrum & Peter, 2011). The difference between the two models is the lines of communications and the levels of authority granted in the organization's units. Preference for an expansive approach based on bringing RM within existing activities or one that is more centralized highlights a preference for leaving the issues around risk to the powers that be which may not impact suitability or an interest in making sure the response to risk is suitable to organizational needs, strategies, and actions (cf. Renn, 2004). The key point is the coordination of activities within an organization to ensure the integrated dualities of performance and performance monitoring, planning and decisionmaking, and evaluation and improvement/enhancement. Decisions tend to be made in terms of trade-offs, in the case of the two models under discussion, it is about locus of control *vis a vis* centrality of authority to make decisions and organizational culture and context, prioritization of issues, and the willingness to expand instead of creating new layers of data collection and analysis and how the information is fed back into the organizational sensemaking mechanism.

Term	COSO Framework	ISO 31000
Risk	The possibility that an event will occur and adversely affect the achievement of objectives	The effect of uncertainty on objectives
Risk appetite	A broad amount of risk an entity is willing to accept in pursuit of its mission or vision.	The amount and type of risk that an organization is willing to pursue or retain.
Risk assessment	Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.	Overall process of risk identification, risk analysis, and risk evaluation.
Risk evaluation		Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.
Inherent risk	Potential for waste, loss, unauthorized use, or misappropriation due to the nature of an activity itself.	
Level of risk		Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.
Risk management	Enterprise risk management is a process, effected by an entity's board of directors, management	Coordinated activities to direct and control an organization with regard to risk.

	and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.	
Risk management framework		Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization
Risk management process		Systematic application of management policies procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring, and reviewing risks.
Residual risk	Risk that remains after management's responses to risk threats, and countermeasures have been applied.	Risk remaining after risk treatment.
Risk response	Management assesses the effect on risk likelihood and impact, as well as costs and benefits, selecting a response that brings residual risk within desired risk tolerances.	
Risk source		Element which alone or in combination has the intrinsic potential to give rise to risk.
Risk tolerance	The acceptable level of variation in performance relative to the achievement of objectives within the context of established laws, regulations, and external standards.	
Risk treatment		Process to modify risk.

sources: AS/NZ ISO 31000: 2009; COSO (2004), COSO (2011), Gjerdrum & Peter (2011), Moeller (2014)

Figure 8. Definitions of risk concepts: COSO Framework and ISO 31000.

Conclusion

Beck (1992) wrote that the modern world is a risk society where risk is a pervasive element of modern life. Power (2007) observed that RM is becoming a sign of the times as it is becoming more frequently part of individual, organizational, political, and social decisionmaking. Not atypically, RM practices in higher education lag in comparison to the corporate world – especially in countries where ERM frameworks have been issued – possibly because it tends to be a top-down approach in a shared government environment reflecting the diversity of activities, interactions, and roles within HEIs (Padró, 2014; Beasley, Clune, & Hermanson, 2005; Huber 2011). The global average of organizations with at least formal risk management procedures in place is about 53% according to a survey from The Institute of Internal Auditors (2015), indicating how RM is still developing as a managerial practice.

Renn (2004) identified four models on how people view and treat risk. One of the models is what RM represents: an early warning indicator through discovery of causal relationships between activities/events and their latent effects. This is not to be confused with risk as a fatal threat resulting from failure or safety concerns, which is part of a different managerial process within HEIs. However, RM represents more as it a structured approach toward identifying and handling issues and their impact at the operational and strategic level if designed properly, thought through as a thinking process, and paid attention to as intended. As Sun Tsu, the Chinese military strategist wrote,

> *In the wise leader's plans, considerations of advantage and of disadvantage will be blended together. If our expectation of advantage be tempered in this way, we may succeed in accomplishing the essential part of our schemes. If, on the other hand, in the midst of difficulties we are always ready to seize an advantage, we may extricate ourselves from misfortune.*

This paper's narrative has identified six concerns and seven questions that HEIs and HEQA should be addressing in their consideration about adopting and/or implementing RM. The questions are:

- What is the purpose for RM? Is it for transparency, systemic risk reduction, risk-return management, or risk as a competitive advantage (e.g., reputation)?

- What models/frameworks should be adopted by an HEI or HEQA? COSO, ISO 31000, ISO 9000, something else?

- How deep into the HEIs should RM be embedded? Should RM be a regulatory compliance reporting mechanism that is performed by an HEI's business unit separate of existing operational and strategic processes? Should RM only be limited to business operations of HEIs and not be fully inclusive of academic and student-related issues?

- What should the RM look like for an HEI or HEQA? How much of it should be a "top-down" versus "bottom-up" scheme?

- Will HEIs and/or HEQA have a preference for an audit-based, bottom-up tick-off the boxes arrangement rather than one of enhancing or shoring up internal accountability

practices? How aligned and integrated will RM be with existing QA and QC processes?

- Is the focus more compliance- and finance-based or will it be more program- and program outcome-based? What will be the key drivers for RM?

- What will be the sector definitions and indicators of risk impacting how RM is designed and implemented by a HEQA or HEIs? What are the policy steering interests and expectations/preferences driving the use of RM by the sector and institutions?

The identified concerns regarding how these questions are answered are:

- RM acting as a force for organisational conservatism rather than as a challenge to enhance organizational practice by identifying opportunity and generating innovative solutions.

- The capacity, experience, and training of staff assessing risks at the HEQA and HEI levels be, especially at the HEQA level performing institutional audit reviews.

- RM becoming a managerial fad that will last a few years and then be replaced with a new approach or scheme, questioning the investment in resources and time commensurate with expected results.

- The QAHE level RM being too burdensome to HEIs, reducing agility, autonomy, and performance in the name of regulatory compliance.

- The blurring between external and internal auditing processes possible under RM and the negative legal impact of compliance making QA and QC processes more cumbersome and less effective.

- RM becoming another institutional silo with its own vocabulary and methodology limiting its integration with mainstream institutional practices.

McNally (2015) and (McNally & Tophoff, 2015, April 1) lists similar concerns to the above, but add the following as duties of care to avoid.

.

- RM and internal control activities becoming objectives in their own right rather than being support tools for the institution's decisionmaking apparatus.

- The RM scheme having a compliance-only mentality.

- The RM scheme treating risk only as a negative.

- The RM scheme not living up to their own RM policies.

The focus of this paper is two-fold: [1] to explain RM from an enterprise (ERM) or institutional perspective and from a regulatory (RRM) perspective and [2] to explore issues pertinent to choices involved in determining whether to adopt RM and how to implement it from the single college or university standpoint and/or from a sector viewpoint. The rationale for the exercise is that RM seems to be an evolutionary development of quality models. RM has been around for a while, with exploratory interests developing in the latter part of the 20th century, often as a result of adverse criminal actions with widespread dilatory social impact. The literature on project management suggests the use of RM to ensure success in complex project environments as well (Harvett, 2013). However, overall what seems to be the driver are the issues of avoiding problems that have a negative impact on the organization and/or sector first, then as a means of determining appropriate practice to mitigate negative effects, and finally a means of identifying opportunities. Because of the impetus for much of the discussion about systematizing risk, there is a policy steering element to it that now has bloomed into legislated or regulatory interests becoming additional drivers into its adoption. With this being the case, the words of another military strategist, Carl von Clausewitz, should be taken into account:

> *If the whole consideration [for war] is a calculation of probability based on definite persons and relations, then the political object, being the original motive, must be an essential factor in the product.*

There are various RM models available for higher education from which to select. The focus here has been on the two models that seem to be most popular, the COSO Framework and the ISO 31000 standard. The questions and concerns discussed throughout this paper help frame the selection process for those HEIs and/or HEQAs interested in adopting RM. The literature suggests that there are not many major differences between the two models presented. Looking at how the various aspects of risk within the models provided here will reflect that. Practitioners in RM even go as far to suggest that the limitations of one model suggest adopting part of the other either to simplify RM or to better explain and flesh out the underlying premises that make RM successful. Context plays a key part in making the decision to adopt and implement RM. For example, context determines the weighing given to qualitative and quantitative evidence as has been discussed above or, as Zhang (2011) observes, treating risk as an objective fact and/or as a subjective construction. As another example, the literature's preference for a "top-down" leadership style for RM and quality processes in general may not work well at some HEIs, particularly at those that are more faculty controlled. The rationale for the "top-down" perspective is that this ensures buy-in, avoids silo thinking and activity thus assists integration of the RM scheme, and provides the basis for a holistic institutional approach in meeting goals and objectives. In an environment where faculty still exert a degree of control, RM needs to also be led from the bottom up in order to engage and provide important roles to those with expertise in an HEI's core technology (Birnbaum, 2003).

To conclude, McNally (2015), lists those characteristics that make up a good RM program, summarizing many of the points previously made in this paper:

- RM is a mechanism to help achieve objectives,
- it should be performance and principles-based,

- tailored to the organization,
- implemented organically,
- integrated and 'built-in',
- dynamic and evolving,
- seen as a sound investment, and
- integrated in governance.

McNally's last point is the important one for higher education because how governance is defined and enacted ultimately decides how RM will look like and actually used. The points addressed in this paper are by no means complete, but should provide a fairly expansive review of the literature and highlight the key points that should help the reader determine how these characteristics can be met by his or her HEI and/or sector.

References

Adam, B., & van Loon, J. (2005). Introduction: Repositioning risk; the challenge for social theory. In B. Adam, U. Beck, & J. van Loon (Eds.), *The risk society and beyond: Critical issues for social theory.* (pp. 1-31). London: SAGE Publications.

Altbach, P.G., & Knight, J. (2007). The internationalization of higher education: Motivations and realities. *Journal of Studies in International Education, 11(3/4),* 290-305.

American Productivity and Quality Center [APQC]. (2007). *Risky business: Employing ERM to sustain growth, mitigate threats and maximize share-holder value*. Houston, TX: Author

Andersen, T.J., Garvey, M., & Roggi, O. (2014). *Managing risk and opportunity: The governance of strategic risk-taking.* Oxford: Oxford University Press.

Arena, M., Arnaboldi, M., & Azzoni, G. (2010). The organizational dynamics of enterprise risk management. *Accounting Organizations and Society, 35,* 659-675.

Association of Governing Boards [AGB]. (2009). *The state of Enterprise Risk Management at colleges and universities today*. Washington, DC: Author. Retrieved from: http://agb.org/sites/agb.org/files/u3/AGBUE_FINAL.pdf.

Astin, A.W., & Antonio, A.L. (2012). *Assessment for excellence.* (2nd ed.). Lanham, MD: Rowman & Littlefield Publishers, Inc.

Australian/New Zealand Standards. (2009). *Risk management – Principles and guidelines: AS/NZ ISO 31000: 2009*. Sydney: Standards Australia and Standards New Zealand.

Australian Universities Quality Agency [AUQA]. (2009). *AUQA Audit Manual, Version 6.0.* Melbourne: Author.

Baird, B. (2010). *Stronger, simpler, smarter ESOS: supporting international students. Final report of the review of the Education Services for Overseas Students (ESOS) Act 2000*. Canberra: Commonwealth of Australia.

Baldrige Performance Excellence Program [BPEP]. (2013). *2013–2014 Education Criteria for Performance Excellence*. Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology.

Basel Committee on Banking Supervision (Basel II). (July 2002). *Sound practices for the management of supervision of operational risk*. Basel: Bank for International Settlements. Retrieved from: http://www.bis.org/publ/bcbs91.pdf.

Beasley, M.S., Clune, R., & Hermanson, D.R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *The Journal of Accounting and Public Policy, 2005, 24,* 521-531.

Beck, U. (2009). Critical theory of world risk society: A cosmopolitan vision. *Constellations, 16(1),* 3 – 22.

Beck, U. (1992) *Risk Society: Towards a New Modernity.* (Trans. M. Ritter). London: SAGE Publishers.

Birnbaum, R. (1988). *How colleges work: The cybernetics of academic organization and leadership*. San Francisco: Jossey-Bass.

Birnbaum, R. (2000). *Management fads in higher education: Where they come from, what they* do, why they fail. San Francisco: Jossey-Bass.

Birnbaum, R. (2003). *The end of shared governance: Looking ahead or looking back*. Paper presented at the Research Forum on Higher Education Governance June 12—14, 2003 in Santa Fé, New Mexico. Retrieved from *http://www.usc.edu/dept/chepa/gov/roundtable2003/birnbaum.pdf*.

Blaskovich, J., & Taylor, E.Z. (2011). By the numbers: Individual bias and enterprise risk management. *Journal of Behavioral and Applied Management, 13(1),* 5-23.

Boas, T.C., & Gans-Morse, J. (2009). Neoliberalism: From new liberal philosophy to anti-liberal slogan. *Studies in Comparative International Development, 44(2),* 137 – 161.

Bradford, J., & Fox, C. (2013). *2013 RIMS Enterprise Risk Management (ERM) Survey*. New York: Risk and Insurance Management Society [RIMS] and Advesen Ltd.

Bradley, D., Noonan, P., Nugent, H., & Scales, B. (2008). *Review of Australian higher education: Final Report*. Canberra: Commonwealth of Australia.

Bugalla, J., Narvaez, K., & Kallman, J. (29 August 2012). Why U.S. Risk managers should take a hint from the rest of the world. CFO. Retrieved from: http://www3.cfo.com/article/2012/8/risk-compliance_erm-coso-iso-31000-narvaez-bugalla.

Charette, R.N. (2010). Enterprise risk management. In P. Simon, (Ed.), *The next wave of technologies: opportunities from chaos.* (pp. 265-283). Hoboken, NJ: John Wiley & Sons.

Charette, R.N. (2012). Enterprise risk management – Supplemental material. In P. Simon, (Ed.), *The next wave of technologies: opportunities from chaos.* Hoboken, NJ: John Wiley &

Sons. Retrieved from http://www.philsimon.com/wp-content/uploads/2009/10/15_Charette.pdf.

Chattopadhyay, P., Glick, W.H., & Huber, G.P. (2001). Organizational actions in response to threats and opportunities. *The Academy of Management Journal, 44(5),* 937-955.

Committee of Sponsoring Organizations of the Treadway Commission [COSO]. (2004). Enterprise risk management – Integrated framework: Application techniques. Durham, NC: American Institute of Certified Public Accountants.

Committee of Sponsoring Organizations of the Treadway Commission [COSO]. (2011). *Internal control – Integrated control.* Durham, NC: American Institute of Certified Public Accountants.

Courtney, H., Kirkland, J., & Viguerie, P. (1997). Strategy under uncertainty. *Harvard Business Review, 75(6),* 66-79.

Curtis, P. & Carey, M. (2012). *Risk assessment in practice*. Committee of Sponsoring Organizations of the Treadway Commission (COSO). Retrieved from http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf.

DeLoach, J. (2012, June 25). *COSO, ISO 31000 or another ERM Framework?* Retrieved from http://corporatecomplianceinsights.com/coso-iso-31000-or-another-erm-framework/

Dionne, G. (2013). *Risk management: History, definition and critique*. Montreal: Interuniversity Research Centre on Enterprise Networks, Logistics and Transportation.

Dow, K.L., & Braithwaite, V. (2013). *Review of Higher Education regulation: Report*. Canberra: Commonwealth of Australia.

Evans, D. (2012). Risk intelligence. In S. Roeser, R. Hillerbrand, P. Sandin, & M. Peterson (Eds.), *Handbook of Risk Theory*. (pp. 603-620). Dordrecht: Springer Science+Business Media B.V.

EYGM Limited & Munich Re. (2015). MENA insurance enterprise risk management survey. London: Author. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-mena-insurance-enterprise-risk-management-survey-2015/$FILE/EY-mena-insurance-enterprise-risk-management-survey-2015.pdf.

Federation of European Risk Management Associations [FERMA]. (2002). *A risk management standard*. Brussels: Author. Retrieved from http://www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-english-vewrsion.pdf.

Feldman, M.S. (2003). A performance perspective on stability and change in organizational routines. *Industrial and Corporate Change, 12(4),* 727-752.

Foucault, M. (2010). *The government of self and others: Lectures at the Collège de France 1982-1983*. (Trans. Graham Burchell). New York: Picador Palgrave McMillan.

Gatzert, N., & Martin, M. (2015). Determinants and value of enterprise risk management: Empirical evidence from the literature. *Risk Management and Insurance Review, 18(1),* 29-53.

Gjerdrum, D., & Peter, M. (2011). The new international standard on the practice of risk management – A comparison of ISO 31000:2009 and the COSO ERM Framework *Risk management, 21,* 8-12.

Groupe Consultatif Actuariel Européen. (2007). *Solvency II glossary*. Brussels: Author. Retrieved from http://ec.europa.eu/internal_market/insurance/docs/solvency/impactassess/annex-c08d_en.pdf.

Grove, J. (2015, June 29). Quality assurance to face overhaul: New system to 'put student needs at the centre'. *Times Higher Education*. Retrieved from https://www.timeshighereducation.co.uk/news/quality-assurance-face-overhaul.

Gryna, F.M. (1999). Operations. In J.M. Juran, A.B. Godfrey, R.E. Hoogstoel, & E.G. Schilling (Eds.), *Juran's quality handbook.* (5th ed.). (pp. 22.1-22.69). New York: McGraw-Hill.

Hardy, K. (2010). *Managing risk in government: An introduction to enterprise risk management.* (2nd ed.). Washington, DC: IBM Center for The Business of Government.

Harvett, C.M. (2013). *A study of uncertainty and risk management practice relative to perceived project complexity.* Unpublished dissertation. Robina, AUS: Bond University.

Higher Education Funding Council for England [HEFCE]. (2005). *Risk management in higher education*. London: Author.

Higher Education Funding Council for England [HEFCE]. (2001). *Risk management: A guide to good practice for higher education institutions.* London: Author.

Hill, C.L., & Booker, Q. (2007). State accountancy regulators' perception of independence of external auditors when performing internal audit activities for nonpublic clients. *Accounting Horizons, 21(1),* 43-57.

Hillson, D. (2004). *Effective opportunity management for projects: Exploiting positive risk*. New York: Marcel Decker, Inc.

Hillson, D., & Murray-Webster, R. (2011). Using risk appetite and risk attitude to support appropriate risk taking: A new taxonomy and model. *Journal of Project, Program & Portfolio Management, 2(1),* 29-46.

Holström, S. (2007). Niklas Luhmann: Contingency, risk, trust and reflection. *Public Relations Review 33,* 255–262.

Holton, G.A. (2004). Defining risk. *Financial Analysts Journal, 60(6),* 19-25.

Hommel, U., & King, R. (2013). The emergence of risk-based regulation in higher education: Relevance for entrepreneurial risk taking by business schools. *Journal of Management Development*, 32 (5), 537-547.

Huber, G.P., & Daft, R.L. (1987). The information environments of organizations. In F.M. Jablin, L.J. Putman, K.H. Roberts, & L.W. Porter (eds.), *Handbook of organizational communication: An interdisciplinary perspective*. (pp. 130-164). Newbury Park, CA: SAGE Publications.

Huber, M., & Rothstein, H. (2013). The risk organisation: or how organisations reconcile themselves to failure. *Journal of Risk Research, 16(6),* 651-675.

Huber, M. (2011). The Risk University: Risk identification at higher education institutions in England. Discussion Paper No: 69. London: London School of Economics and Political Science.

Hutter, B., & Power, M. (2005). Organizational encounters with risk: an introduction. In B. Hutter & M. Power (Eds.), *Organizational encounters with risk.* (pp. 1-32). Cambridge, UK: Cambridge University Press.

Institute of Internal Auditors [IIA]. (2013). *International Professional Practices Framework (IPPF), 2013 Edition*. Altamonte Springs, FL: The IIA Research Foundation.

Institute of Internal Auditors [IIA]. (2008). *Sarbanes-Oxley Section 404: A guide for management by internal control practitioners*. (2nd ed.). Altamonte Springs, FL: Author.

Jablonowski, M. (2007). Avoiding risk dilemmas using backcasting. *Risk Management, 9,* 118–127.

Jasanoff, S. (1993). Bridging the two cultures of risk analysis. *Risk Analysis, 13(2),* 123-129.

Juran, J.M., & Godfrey, A.B. (1999). The quality control process. In J.M. Juran, A.B. Godfrey, R.E. Hoogstoel, & E.G. Schilling (Eds.), *Juran's Quality Handbook* (4.1-4.29). (5th ed.). New York: McGraw-Hill.

Knight, F.H. (1921). *Risk, uncertainty, and profit.* Boston: Houghton Mifflin Company.

Langevoort, D.C. (2006). Internal controls after Sarbanes-Oxley: Revisiting *Corporate Law's* "duty of care as responsibility for systems." *Journal of Corporation Law,* 31(3), 949-973.

Leech, T.J. (2012). *The high cost of "ERM herd mentality": White Paper.* Oakville, Ontario: Risk Oversight. Retrieved from http://riskoversightsolutions.com/wp-content/uploads/2011/03/Risk_Oversight-The_High_Cost_of_ERM_Herd_Mentality_March_2012_Final.pdf.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47(2),* 263-292.

Kaplan, R.S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review, 90(6),* 48-60.

Kaplan, R. S. (2009). Risk management and the strategy execution system. *Balanced Scorecard Report in Harvard Business Publishing Newsletters, 11(6),* 3–8. Retrieved from http://www.exed.hbs.edu/assets/Documents/riskmanagement-strategy.pdf.

Kaplan, R.S., & Norton, D.P. (1996). Strategic learning and the balanced score card. *Strategy & Leadership, 24(5),* 18 – 24.

Luhmann, N. (1993). *Risk: A sociological theory.* (Trans. R. Barrett). Berlin: Walter de Gruyter.

March, J.G., & Olsen, J.P. (1975). The uncertainty of the past: Organizational learning under ambiguity. *European Journal of Political Research, 3,* 147-171.

Marks, N. (2011, February 21). 10 reasons not to like the COSO ERM framework – a discussion with Grant Purdy. *Norman Marks on Governance, Risk Management, and Audit.* Retrieved from https://normanmarks.wordpress.com/2011/02/21/10-reasons-not-to-like-the-coso-erm-framework-%E2%80%93-a-discussion-with-grant-purdy/

Marsh Canada LTD. (2012). Risk in Canada's higher education landscape: A survey of Canadian universities and colleges. Toronto: Author. Retrieved from http://www.collegecentreofboardexcellence.ca/PDFs/Risk%20in%20Canada%27s%20Higher%20Education%20Landscape%20-%20Marsh%20-%20Feb%202011.pdf

Martin, D., & Power, M. (2007). The end of enterprise risk management. *AEI-Brookings Joint Center for Regulatory Studies*. Washington, DC: Brookings Institute.

Massaro, V. (2013). TEQSA and the holy grail of outcomes-based quality assessment. In S. Marginson (Ed.), *Tertiary education policy in Australia*. (pp. 49-58). Melbourne: University of Melbourne Centre for the Study of Higher Education.

McNally, J.S. (2012, June 26). *COSO Framework holding strong – Getting a polish.* Retrieved from http://www.accountingweb.com/practice/practice-excellence/coso-framework-holding-strong-getting-a-polish.

McNally, J.S. (2015). Risk: Leverage it. Control it. Win! *Pennsylvania CPA Journal, 85(4),* 26-30.

McNally, J.S., & Tophoff, V. (2015, April 1). Stacked in your favour. *Strategic Finance*. Retrieved from http://sfmagazine.com/post-entry/j-stephen-mcnally-cpa-vincent-tophoff-ra/.

Miles, R.E., & Snow, C.C. (1978). *Organizational strategy, structure, and process*. New York; McGraw-Hill.

Milliken, F.J. (1987). Three types of perceived uncertainty about the environment: State, effect, and response uncertainty. *Academy of Management Review, 12(1),* 133-143.

Mikes, A. (2005). *Enterprise risk management in action. Discussion paper no. 35*. London: The London School of Economics and Political Science. Retrieved from http://www.lse.ac.uk/accounting/CARR/pdf/dps/disspaper35.pdf.

Mikes, A., & Kaplan, R.S. (2015). When one size doesn't fit all: Evolving directions in the research and practice of enterprise risk management. *Journal of Corporate Applied Finance, 27(1),* 37-40.

Mitchell, S.L., Switzer, C.S., & Mefford, J. (2015). *OCEG Red Book GRC Capability Model: Achieving principled performance by integrating the governance, assurance and management of performance, risk and compliance. Version 3.0-EXPOSURE.* Scottsdale, AZ: OCEG.

Moeller, R.R. (2014). *Executive's guide to COSO internal controls: Understanding and implementing the new framework.* Hoboken NJ: John Wiley & Sons, Inc.

National Association of College and University Business Officers [NACUBO]. (November 2003) The Sarbanes-Oxley Act of 2002: Recommendations for higher education. *Advisory Report,* 2003-3, 1-11. Retrieved from http://www.nacubo.org/documents/news/2003-03.pdf.

National Institute of Standards and Technology [NIST]. (2010). *Guide for applying the risk management framework to Federal Information Systems: A security life cycle approach.* NIST Special Publication 800-37 Revision 1. Gaithersburg, MD: Author. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

O'Shea, M., & Krischanitz, C. (2013). *Comparison of the regulatory approach in insurance and banking in the context of Solvency II.* Brussels: Groupe Consultatif Actuariel Européen. Retrieved from http://actuary.eu/documents/SII%20vs%20Basel%20II_Dec_12_final.pdf.

Padró, F.F. (2014). A conceptual framework on establishing a risk management framework within existing university assessment and evaluation practices, *Studies in Learning, Evaluation, Innovation and Development, 10(1),* 1-13.

Padró, F.F. (2010). *An early call for increased oversight by state boards of higher education: A case study from New Jersey*. Paper presented at the 35th Annual ASHE Conference, 18-20th November, 2010, Indianapolis, IN.

Padró, F.F. (1988). *Quality Circles and Their Existence in Present-Day School Administration*. Unpublished dissertation. Tucson, AZ: University of Arizona.

Padró, F.F., & Kek, Y.C.M.A. (2013). *Student engagement and student satisfaction: Two measures arguing for independent review criteria of standards for student support services in national quality assurance schemes*. Paper presented at the 2013 Biennial INQAAHE Conference, Taipei, Taiwan, 9-11 April 2013.

Padró, F.F., Winwood, N., & Hawke, M.F. (2015). *Utilizing qualitative components of risk management as evidence on how university strategies meet QA criteria and standards.* Paper presented at 2015 INQAAHE Biennial Conference March 30 – April 3, 2015, Chicago, IL, USA.

Pascale, R.T. (1999). Surfing on the edge of chaos. *Sloan Management Review, 40(3),* 83-94.

Percy, A. & Beaumont, R. (2008). The casualisation of teaching and the subject at risk. *Studies in Continuing Education*. 30 (2), 145-157.

Pergler, M. (2012). *Enterprise risk management: What's different in the corporate world and why. McKinsey Working Papers on Risk, Number 40*. New York: McKinsey & Company.

Pfeffer, J., and Salancik, G.R. (1978). *The external control of organizations*. New York: Harper & Row.

Power, M. (2007). *Organized uncertainty*. Oxford, UK: Oxford University Press.

Project Management Institute. (2013). *A guide to the project management body of knowledge (PMBOK® Guide)*. (5th ed.). Newton Square, PA: Author.

Protiviti. (2013). *The updated COSO Internal Control Framework: Frequently asked questions.* (2nd.ed.). New York: Author. Retrieved from http://www.protiviti.com.au/en-US/Documents/Resource-Guides/Updated-COSO-Internal-Control-Framework-FAQs-Second-Edition-Protiviti.pdf.

Queensland Government. (2011). *A guide to risk management*. Brisbane. Author. Retrieved from https://www.treasury.qld.gov.au/publications-resources/risk-management-guide/guide-to-risk-management.pdf.

Rao, S., & Goldsby, T.J. (2009). *Supply chain risks: a review and typology. The International Journal of Logistics Management, 20(1),* 97 – 123.

Renn, O. (2004). Perception of risk. *The Geneva Papers on Risk and Insurance, 29(1),* 102-114.

Riesch, H. (2012). Levels of uncertainty. In S. Roeser, R. Hillerbrand, P. Sandin, M. Peterson (Eeds.), *Handbook of Risk Theory*. (pp. 88-111). Springer Science+Business Media B.V.

Rittenberg, L. & Martens, F. (January 2012). *Understanding and communicating risk appetite*. Chicago: COSO. Retrieved from http://www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf.

Senge, P.M. (2006). *The fifth discipline: The art & practice of the learning organization*. (Revised ed.). New York: Currency Doubleday.

Shenkir, W.G., & Walker, P.L. (2007). *Enterprise risk management: Tools and techniques for effective implementation.* Montvale, NJ: Institute of Management Accountants.

Spikin, I.C. (2013). Risk management theory: The integrated perspective and its application integration in the public sector. *Estado, Gobierno, Gestión Pública, 21,* 89-126.

Stake, R.E. (1967). The countenance of educational evaluation. *Teachers College Record, 68,* 523-540.

State of New Jersey's Commission of Investigation (SCI). (2007). *Vulnerable to abuse: The importance of restoring accountability, transparency, and oversight to public higher education governance.* Trenton, NJ: Author. Retrieved from http://www.state.nj.us/sci/pdf/HigherEdFinalReport.pdf.

Stufflebeam, D.J. & Coryn, C.L.S. (2014). *Evaluation theory, models, & applications*. (2nd ed.). San Francisco: Jossey-Bass.

Tapper, E.R., & Salter, B.G. (1998). The Dearing Report and the maintenance of academic standards: Towards a new academic corporatism. *Higher Education Quarterly, 52(1),* 22-34.

Taylor, P.R. (2012). The mismeasure of risk. In S. Roeser, R. Hillerbrand, P. Sandin, & M. Peterson (Eds.), *Handbook of Risk Theory*. (pp. 441-475). Dordrecht: Springer Science+Business Media B.V.

Tertiary Education Commission. (2014). *Statement of Intent 2014-2018.* Wellington, NZ: Author. Retrieved from http://www.tec.govt.nz/Documents/Publications/TEC-Statement-of-Intent-%28SOI%29-2014-2018.pdf.

Tertiary Education Quality and Standards Agency Act 2011. Retrieved from https://www.comlaw.gov.au/Details/C2013C00169/Download.

Tertiary Education Quality and Standards Agency (TEQSA). (2012). *Regulatory risk framework.* Retrieved from *h*ttp://www.teqsa.gov.au/sites/default/files/TEQSARegulatoryRiskFramework_0.pdf.

Tertiary Education Quality and Standards Agency (TEQSA). (2014). *TEQSA's risk assessment framework version 2.0*. Retrieved from http://www.teqsa.gov.au/sites/default/files/publication-documents/TEQSARiskAssessFramework2014_1.pdf.

The Institute of Internal Auditors [IIA]. (2015). *2015 Global pulse of internal audit: Embracing opportunities in a dynamic environment*. Altamonte Springs, FL: Author.

Tian, J. (2004). Quality-evaluation models and measurements. *IEEE Software, 21(3),* 84–91.

Toney, J.M., Jr. (n.d.). Integrating quality, safety and risk to improve performance. Retrieved from http://www.asq-qm.org/resourcesmodule/download_resource/id/371/src/@random4baa4bfa00315/.

Tufano, P. (2011). Managing risk in higher education. *Forum Futures 2011 EDUCAUSE,* 54-58.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science 30(4481),* 453-458.

United Nations Economic Commission for Europe. (2012). *Risk management in regulatory frameworks: Towards a better management of risks.* New York and Geneva: Author. Retrieved from http://www.unece.org/fileadmin/DAM/trade/Publications/WP6_ECE_TRADE_390.pdf.

United States Government Accountability Office. (2011). Government Auditing Standards: 2011 revision. Washington, D.C.: Author. Retrieved from http://www.gao.gov/assets/590/587281.pdf.

University of Adelaide. (n.d.). *Risk Management Handbook.* Adelaide: Author. Retrieved from http://www.adelaide.edu.au/legalandrisk/docs/resources/Risk_Management_Handbook.pdf.

Vandenberg, A., & Hundt, D. (2012). Corporatism, crisis and contention in Sweden and Korea during the 1990s. *Economic and Industrial Democracy, 33(3),* 463–484.

Weick, K.E., Sutcliffe, K.M., & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. *Organization Science, 16(4),*409-421.

Weick, K.E. (1995). *Sensemaking in organizations*. Thousand Oaks, CA: SAGE Publications.

Wueest, B., & Fossati, F. (2015). Quantitative discursive institutionalism: a comparison of labour market policy discourse across Western Europe. *Journal of European Public Policy, 22(5),* 708-730.

Zachman, K. (2014). Risk in historical perspective: Concepts, contexts, and conjunctions. In C. Klüppelberg, D. Straub, & I. Welpe (Eds.), *Risk - A multidisciplinary introduction.* (pp. 3-35). Heidelberg: Springer International Publishing Switzerland.

Zhang, H. (2011). Two schools of risk analysis: A review of past research on project risk. *Project Management Journal, 42*(4), 5-18.

Zinn, J.O. (2010). Risk as discourse: Interdisciplinary perspectives. *Critical Approaches to Discourse Analysis across Disciplines, 4(2),* 106-124.