A conceptual framework on establishing a risk management framework within existing university assessment and evaluation practices

by

Fernando F. Padró[1]
Senior Lecturer (Quality)
University of Southern Queensland
fernando.padro@usq.edu.au

Abstract

Introducing risk management as an integrated component of university governance and administrative structures is still at a developmental phase because of the relative newness of the concept and the approach to it taken by TEQSA. Most of the experience is at the external governance level and in certain aspects of university administrative practice. This paper addresses the questions of what does a risk management framework look like at a university, how far down the organisation does a risk framework have to be incorporated into existing performance monitoring and reporting apparati and how it can be done. In light of a lack of specific examples in the current literature, the questions are addressed through the presentation of a conceptual framework describing issues that need to be considered and included in creating a risk management process.

Key words

COSO, enterprise risk management (ERM), ISO 31000, TEQSA Regulatory Risk Framework

Introduction

> *A risk is a chance you take; if it fails you can recover. A gamble is a chance taken; if it fails, recovery is impossible.*
>
> Erwin Rommel

Risk is becoming the new paradigm in quality assurance in higher education. As WWII German Field Marshal Rommel pointed out, identifying and dealing with risk provides an opportunity for recovery. Not acknowledging risk and making it part of assurance and framework schemes can lead to some actions treated as a gamble because of the lack of an explicit calculus identifying actions, consequences of actions and options based on the impact of consequences. This paper covers reasons why risk management is a preferred tool of a regulatory environment plus discusses different models and how their approach to defining risk and related terms focusing on different aspects of risk influence how to establish a risk management scheme. Questions of how a risk management framework looks like within a university, how far the university should it drill down to and what the scheme looks like are addressed.

[1] Author's version of paper presented at Australasian Higher Education Evaluation Forum Annual Conference, 28-29 Oct 2013, Launceston, Tas. (Unpublished).

Background

Risk management combines aspects of quality assurance (QA) and quality control (QC) within a university. Both QA and QC evaluate actual performance, compare performance to goals (outcomes), and take action on the difference. However, QA assures those outside a unit that the unit is doing a good job while QC is based on feedback loops (process controls) that monitor performance stability through conformance to standards (Juran, 1999; Juran & Godfrey, 1999). QC 'is one of the three basic managerial processes through which quality can be managed' (Juran & Godfrey, 1999, p. 4.2), with the other two being quality planning and quality improvement. The model of enterprise risk management (ERM), as enacted by the Tertiary Education Quality and Standards Agency (TEQSA), assures that university QC mechanisms are doing the job right through monitoring for identified key risk factors. ERM also acts a control mechanism because the key risk factors are indicators that must demonstrate conformance to accepted parameters defining successful risk management.

Link between ERM and regulatory environments

Michael Power's (2007) observation that business risk assessment is both a symptom and definer of the times is one that has to be taken to heart by universities and their units as these notions are more frequently shape organisational behaviour at the external governance, university corporate and unit levels. Dow and Braithwaite's (2013) review of TEQSA makes this point all the more important. ERM is shaping QA in higher education primarily in Australia, the UK and the USA directly and indirectly. The reason for this Power's (2012) utilisation of Foucault's (1980) definition of apparatus that suggests that practices such as risk management sooner or later transcend the macro-micro, external-internal, and local-central dichotomisation of organisational behaviour because of the blending or blurring of law and management characteristics, particularly in a neoliberal environment. Specifically, as Foucault (2008/1978-1979) pointed out, "[a]n enterprise society and a judicial society, a society orientated towards the enterprise and a society framed by a multiplicity of judicial institutions, are two faces of a single phenomenon" (p. 150). Thus, instead of looking at where separation exists, risk framework is better looked at from the perspective of contingent variables influencing control system design and implementation such as alignment, culture, environment, leadership, size, strategy, structure and technology (Woods, 2009; Drew, Kelly, & Kendrick, 2006). And while at it, another contingent variable at play is the practical impact of the ontological difference between the definitions used to define and operationalise risk, risk frameworks, enterprise/strategic risk management, and related concepts.

Downer (2011) makes an interesting argument about the impact of determining the reliability of performance being proportionate to the impact of that performance on society. For 'mundane' artefacts, the practices of QC are very adequate, but for complex technologies, assessments must be prospective so that their reliability is known before deployment, making measurement highly consequential. However, he also argues that there is a distortive effect that can lead to perverse consequences based on calculative tools transfiguring practices 'in unexpected ways and with unanticipated consequences…' (p. 270). As long as education is deemed to have high impact on society, a regime of what Foucault (2008/1978-1979) called

governmentality prevails because interests of sovereignty currently suggest regulation based on the transactional exchange (cf. Luhmann, 1995/1984) between universities and governmental bodies to ensure the normative values represented by the governing bodies are reflected in institutional practice (Landecker, 1951). The *raison d' etre* is to avoid or mitigate a university that Birnbaum (1988) termed an anarchic organisation characterised by unaccounted and unresolved problems of ambiguous, hence, problematic goals; the presence and use of unclear technology within characteristic institutional process that end up impeding the documented conversion of inputs (resources) to outputs (student learning outcomes); and fluid participation, where decisions are made in a fragmentary rather than participatory and systemic manner. A risk framework within a regulatory environment therefore acts as a technology of government "to create the responsible and calculating individual' (Miller, 2001, p. 380) to as many social entities as possible and why Power (2007) concludes that risk assessment is part of both auditing and regulating activities. It defines and aligns priorities, providing context within organisational evaluative activities (e.g, Stufflebeam's CIPP – context, input, process, product, Stufflebeam & Shinkfield, 2007) and helps set up tolerance for variation based on process control through reliable data collection- and analysis-supported strategic approaches and identifying and managing risk to compensate for uncertainty.

TEQSA's Regulatory Risk Framework (RRF) presents a challenge to universities regarding how far down the organisation a risk management scheme should go. As per the TEQSA website (http://www.teqsa.gov.au/regulatory-approach/regulatory-risk-framework), the RRF is designed as a tool to support its internal decision-making. It 'is not intended for use by providers as a risk management tool' (TEQSA, 2012, p. 4) because TEQSA does not want to mandate unnecessary processes. But as Tufano (2011) pointed out, risk management practices in higher education lag in comparison to the corporate world, with a potential difficulty in implementing them being shared governance systems and the distributed decision-making structures that exist within a university environment. This is due to the internal tension inherent in the existence of two different but with equally valid claims and systems for organisational controls and influence: legal authority as vested in the corporate board and administration and the academic staff grounded on professional authority (Birnbaum, 2003) based on disciplines and professions. The notion of *shared governance* is meant to act as a check and balance mechanism in support of better decision making although changes in technologies and distance education have extended the realm of academic activity governed mainly though managerial initiative (Westmeyer, 1990; Del Favero, 2002; Rhoades, 2003). This is one reason why in n the USA for example, 60 per cent of respondents in a survey by the Association of Governing Boards (AGB) and United Educators (2009) indicated their institutions did not use comprehensive risk assessment, with only five per cent of respondents indicating their institutions have 'exemplary practices' for risk assessment. However, the expectation is that universities develop and assess the appropriateness and impact of their internal risk management systems.

Different approaches to ERM

Universities in Australia are aware that TEQSA's use of a risk framework is legislative based, with the original premise set by its predecessor the Australian Universities Quality

Agency (AUQA). However, there are different definitions of risk and risk frameworks that provide the conceptual framework for divergent approaches toward establishing a risk framework. TEQSA has its own definition as the basis of establishing its operational perspective and comparing TEQSA's definitions with those of the competing frameworks is the first place to begin when considering the creation of a university's risk schema.

TEQSA's definition of regulatory risk *'refers to 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)*' (TEQSA, 2012, p. 34). Risk from an operational perspective is similar, except the focus is on loss, as exemplified in the Basell II (2002) definition of operational risk. Risk itself has remained a somewhat stable definition so far in the 21st century, grounded on defining risk as a function of *likelihood* and *impact* (Curtis & Carey, 2012). For example, the Federation of European Risk Management Associations (FERMA, 2002) adopted the ISO/IEC Guide 73 definition of risk as an uncertain future outcome that can either improve or worsen position that has now been superseded by the ISO 31000 (2009) Standard that simplifies the definition to the effect of uncertainty on objectives. Similarly, the Risk and Insurance Management Society (RIMS, 2012) defines risk as an uncertain future outcome that can either improve or worsen position while the Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2013) continues to define risk in a comparable manner: the possibility that an event will occur and adversely affect the achievement of objectives. However, within these definitions there are two overall approaches espoused in the literature and defined standards by differing organisations that can be applied to forming a risk management framework within a university. One approach is the one currently promoted by COSO which reflects the Basel II definition. This methodology is internal control driven, with activities constructed to look at the degree of organisational compliance to a defined set of standards or expectations. The second approach is based on the ISO 31000 standard that embeds risk within an organisation's QA and QC schema to counteract and explicitly address uncertainty. 'The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organisation at all levels' (ISO 31000, 2009, p. 8).

The difference between the two approaches comes from the outlook they espouse. Bugalla and Narvaez (2012) point out that COSO focuses on the downside, the possibility that an event will adversely affect the achievement of objectives while ISO 31000 looks at the positive side, with risk as an outcome of uncertainty regarding objectives. They also argue that there is a difference based on how legitimate internal audits can be, with a preference given to ISO 31000 because of its clear statement that management should embed ERM into the strategic planning process and allows for internal audit and compliance control elements to evaluate performance.

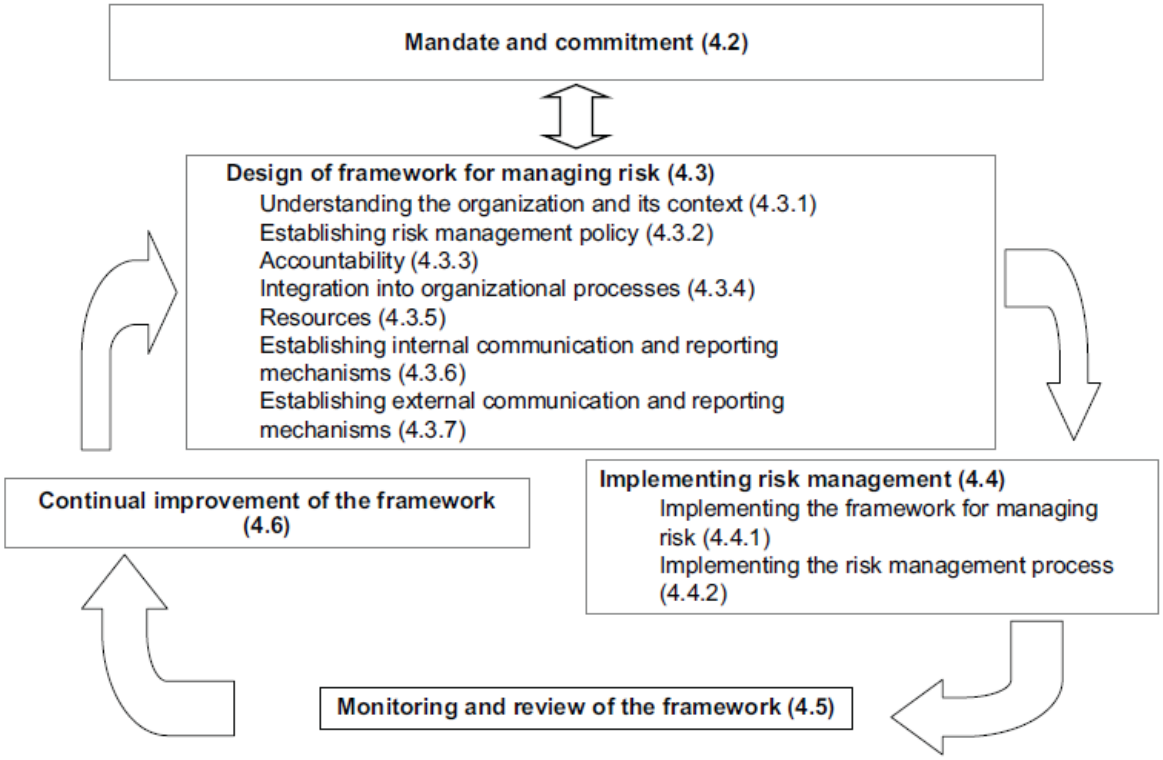
COSO looks at risk from the perspectives of loss and mitigation on the ability to achieve objectives and outcomes. Its focus is on risk appetite and the elements of risk appetite (risk profile, risk capacity, risk tolerance and desired level of risk – Rittenberg & Martens, 2012). RIMS (2012) defines risk appetite as a risk return trade-off for achieving one or more desired

and expected outcomes. The emphasis is more strategic in nature emphasising strategic planning and institutional integrity through mitigating unfavourable events and/or results. Its mantra is the notion of fiscal control management, with its components being risk assessment, risk response, control activities, information and communication, and monitoring from the strategic, operations, reporting, and compliance perspectives. These have to be viewed holistically (O'Donnell, 2005); however, COSO looks for activities to exist at the institutional, faculty, department, and individual program levels. Internal control only is a means to an end due to its ongoing, dynamic and iterative nature (COSO, 2013). The limelight of the internal control processes is placed on the people within the organisation, their ability to be accountable and perform in an ethical manner, their capability to achieve objectives to meet needs in different but at times overlapping categories, and their ability to be adaptable within the organisational structure to meet needs.

ISO 31000 looks at and handles risk from the standpoint of risk having positive as well as negative consequences. The focus is not on risk appetite (which is not part of ISO 31000); rather, it is more on:

- Creation and protection of value;
- Being an integral part of all [organizational] processes;
- Being part of decisionmaking;
- [Having] capacity to explicitly address uncertainty;
- Being systematic, structured and timely;
- Basing decisions on best available information;
- [Tailoring process] to the institution – [making it the university's own];
- Transparency and inclusiveness;
- [Being] dynamic, iterative and responsive to change; and
- [Facilitating the organisation's] continual improvement (ISO 31000, 2012, pp. 7-8).

One important element of the risk framework under ISO 31000 is its embedding risk management into the traditional QA components found within a university, its comfort with the classic Plan-Do-Check-Act cycle and prominence it gives to continuous improvement as exemplified in Figure 1 below. This is in contrast to the COSO Framework which, according to Protivity (2006), that looks at quality initiatives as tools that provide the tools to look at the efficiency and quality of process from a detailed rather than strategic outlook. There are synergies between the two approaches, but quality processes such as Six Sigma, for example, are too operations oriented and lose the big picture perspective. If ERM gets embroiled at this level of detail, Protivity suggests the application of risk becomes 'too detailed and cumbersome' (p. 106). This point-of-view poses a legitimate challenge toward implementing a risk framework because it does contradict the stated desire to avoid cumbersomeness, avoid needless duplication of effort, use existing resources and allow for ease of implementation and use. A university has to determine the approach it wants to take in establishing a risk framework based on two partially divergent models and on the capacity it has to combine risk management with existing QA and QC processes or to add an additional layer to its assessment and evaluation activities that make up various governance structures at the institutional, faculty, unit and program levels.



source: ISO, 2009, p. 9

Figure 1. Relationships between the components of the ISO 31000 framework for managing risk

University risk management framework

Porter (1996) argues that the root of the problem organisations have competing in a highly changing environment is failure to distinguish between operational effectiveness and strategy. Efforts based on techniques to improve quality performance have not translated gains in this area into sustainable gains – profitability. Porter's view has to be framed in Wood's (2009) suggestion that national and international governance regulations that are developing or in place see corporate governance, internal control and risk management as interdependent, probably as a means of creating trust in the assurance process (cf. Jeacle & Carter, 2011). Herein enters the challenge of the reliability of the technology in assessing and evaluating these matters as already pointed out earlier in this paper as well as the associated costs of meeting the regulatory demand for compliance and reporting (Wildavsky, 1972).

There are two primary interests driving the external demand to have universities formulate a more risk-based approach to institutional QA: improving response to student needs (Department for Business Innovations & Skills, 2011) and collect credible, quality information about university performance based on proportionality (TEQSA, 2012) between external demands for accountability and institutional autonomy.

Regardless of approach a university wants to take – and to a lesser extent the units within the institution – COSO's (2011) approach to establishing ERM applies:

- Support from the top;
- Using incremental steps and use a 'small wins approach to achieve immediate, tangible results;
- Initially focus on a small number of top risks, possibly only in one unit;
- Build on existing risk management activities such as those performed for internal audit and compliance functions or other related activities;
- Embed ERM into the university's business fabric – integrated rather than as a stand-alone process; and
- Provide updates and continuing education opportunities (especially for senior leaders).

From an institution-wide point-of-view, COSO's (2011) initial steps also act as a useful guideline to get the process started.

- Seek board and senior leadership, involvement and oversight.
- Select a strong leader to drive the ERM initiative.
- Establish a management risk committee or working group.
- Conduct an initial institution-wide risk assessment and develop an action plan.
- Inventory the existing risk management practices.
- Develop an initial risk reporting mechanism.
- Develop the next phase of action plans and ongoing communications.

Where it becomes tricky is whether implementation occurs at the external (corporate board and senior leadership) or internal governance structures (Academic Board, etc.). Most examples of where risk management is applied through legislation or regulation is concerned with external governance (e.g., National Association of College and University Business Officers [NACUBO], 2003; Higher Education Funding Council for England [HEFCE], 2001). Hence, most Australian universities if the University of Southern Queensland is a typical example, are responding in a manner consonant to COSO's approach, but the question is how and how far to drill down risk management activities and decisions within a university's existing internal governance structure. TEQSA does not want to impose such a regime, but the impetus behind risk management suggests that it is a good idea.

Bringing risk management down to the Faculty, unit and program level

There is little in the literature regarding risk management in higher education; therefore, other than the example of external governance as practiced in the USA and UK. In fact, it can be cogently argued that risk management is a relatively new concept, really getting its legs in the 1990s (Power, 2007). This also means that there are few examples that have been shared in the literature and what follows is a framework to guide decisions on attempting to incorporate risk management into existing QA and QC functions rather than adding a new set of processes.

Figure 2 provides a basic framework on how risk assessment fits within an evaluation scheme that is part of both the QA and QC processes at the institutional as well as internal unit levels of a university. Risk in this framework works as a means of identifying what's going on and what needs to be done, strategising and prioritising based on outcomes and an understanding of what can happen if outcomes are not met. A typical feedback loop tends to reflect Argyris and Schön's (1974) double loop learning based on confirmation and/or disconfirmation of

outcomes. Risk is a knowledge component – questions that need to be answered – in this framework located in the lower row, hence a significant aspect of how things at a university or within a specific Faculty or unit are assessed and evaluated. The top row are those strategic generating elements – resources, context, leadership, structures, politics and environmental scanning capabilities – that help frame and enact the strategy.

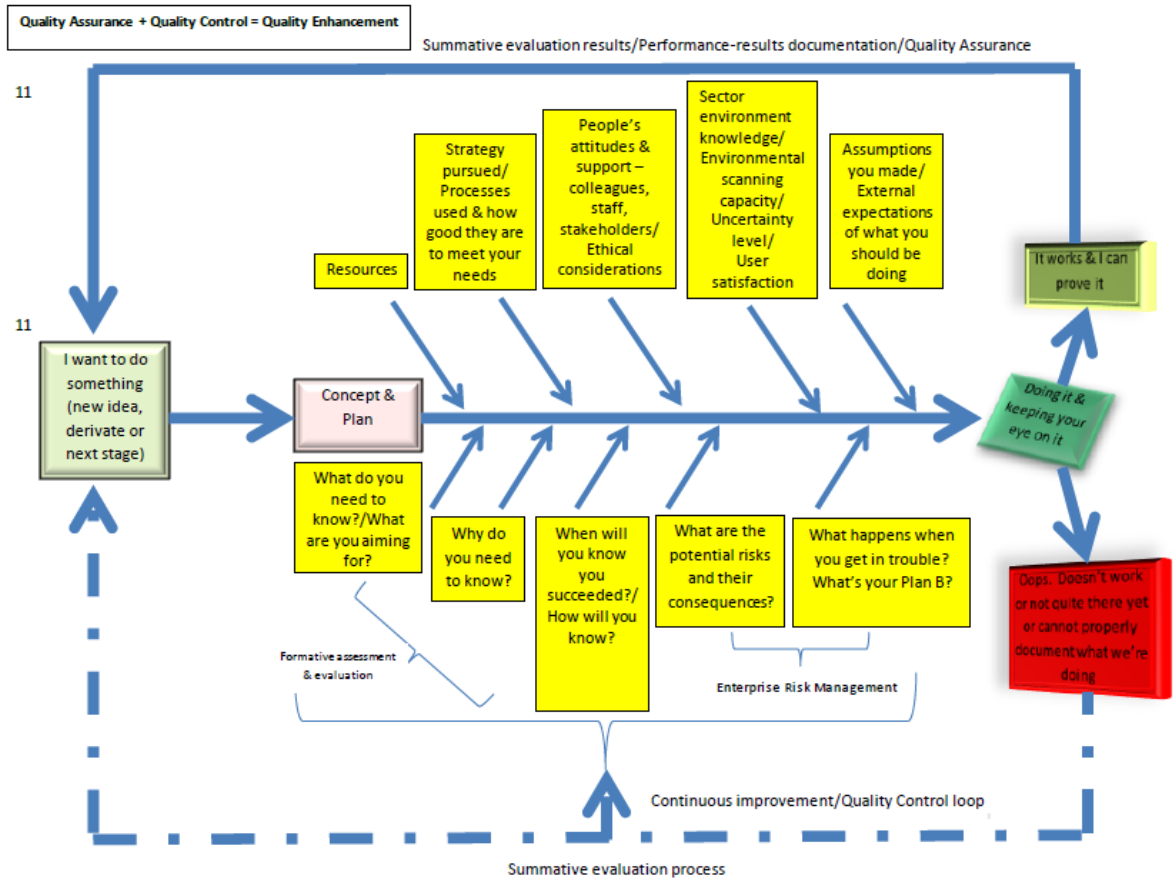


Figure 2. Framework for institutional and unit level QA and QC assessment and evaluation activities

Although not an end-all, one of the drivers of this process is the use of key performance indicators (KPIs) which, in turn are then made into key risk indicators (KRI) (Figure 3). Key performance indicators (KPIs) look at historical performance activity whereas key risk indicators (KRIs) concentrate on real-time indicators offering information about emerging risks (Scarlat, Chirita, & Bradea, 2012). The difference between the two is that KPIs tell whether goals are met while KRIs help 'understand changes in risk profile, impact and likelihood to achieve… goals' (p. 7). These KPIs and KRIs are then set up alongside an assessment element that helps inform a university's overall and unit performance evaluation, improvement activities and planning. KPIs and KRIs should include inputs from the different types of available data to make a more complete and thorough set of indicators: survey results, internal (unit): databases, institution databases used for planning and reporting purposes, student performance data (grades, outcome achievement), graduate and other stakeholder data if available. TEQSA risk indicators then act as both framers and evaluative elements of the process. For example, when the focus is on students and academic staff performance, under the 2012 iteration of TEQSA RRF, a university would want to use the following factors to frame and evaluate: Declining publications (D4), Enrolment (B1, F1, F3), Retention (F4), Persistence (F5), Low HDR completion rate (D6), Admissions standards

(F2), Satisfaction (F6, F7, F8), Employment (F8) and Weak QA/QC program (D9). Other related KPIs and KRIs in these areas could be graduation rates and time of degree completion.

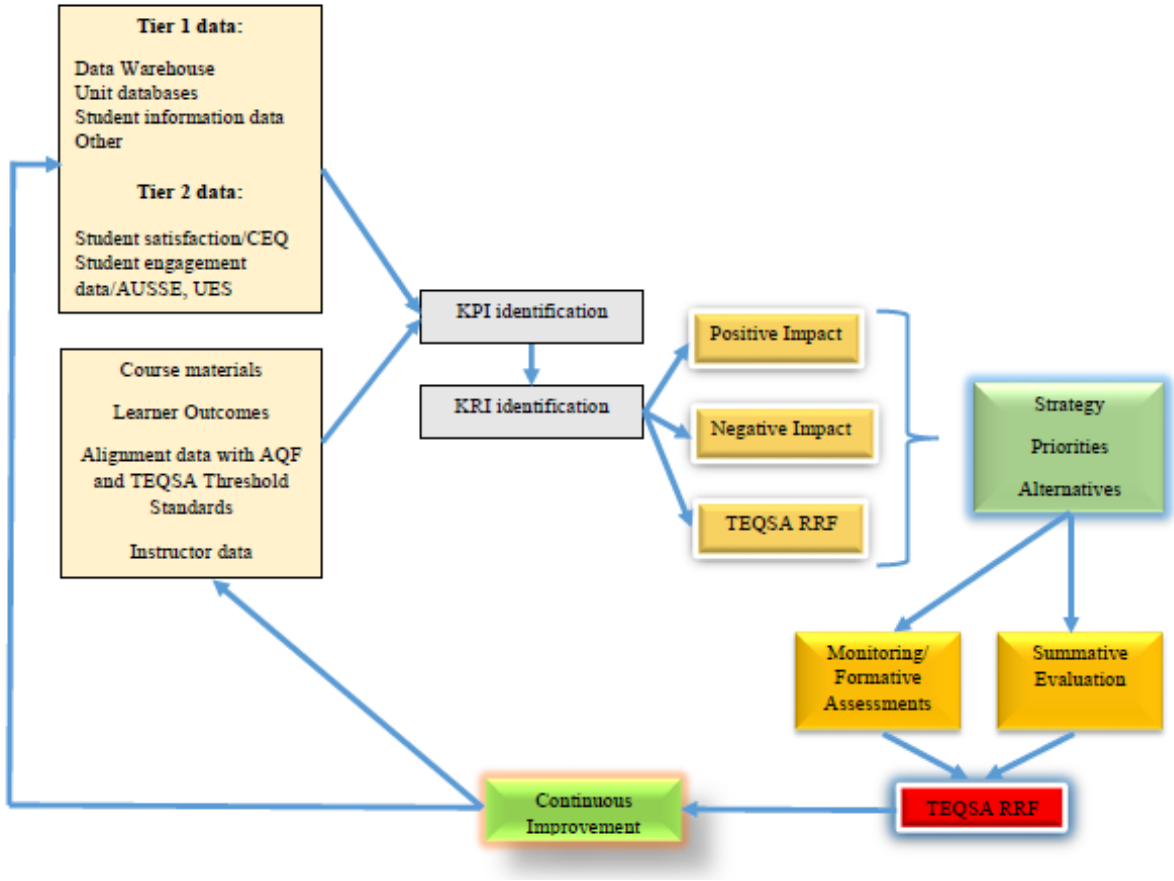


Figure 3. Setting of KPI and KRI within QA and QC processes

The framework applies to an institution-wide risk framework as well as to one adopted by varying unit levels within a university. Based on previous comments in this paper, the primary push for risk management is at the institutional level, focusing on external governance, planning units and, to a limited extent, internal governance. The reason for this is TEQSA's interest in looking at regulatory risk management to capture university data to determine if formal regulatory intervention is needed framed by the three concerns of risk to students, risk to reputation and risk of provider collapse. This view is consistent with findings in the USA where only 36 per cent of public institutions and 17 per cent of private institutions indicated that their campus had already performed assessments of their internal controls (NACUBO, 2005). The early strategy seems to focus on how a university is able to document its performance in relation to the different risk categories. A consequence of this is the deprioritizing, belaying or ignoring the appropriateness of drilling down these activities to the different unit levels within the campus structure. One difficulty raised by the omission in vision regarding the drill-down is that there is a strong potential to not bridge risk management data collection and analysis activity with other similar activities on campus that undergird QA and QC at those levels. This gap raises its own risk that there may not be a seamless process or set of processes regarding risk management that can be applied at all levels to help focus expectations, outcomes, strategies and results. A second more significant risk resulting from the gap however, is not establishing similar criteria in developing KRIs

and aligning unit KRIs with those of the university, creating a probability of increased reporting burdens and strategic responses.

Conclusions

Dow and Braithwaite (2013) document complaints from the higher education sector that TEQSA has added to the reporting burden. There is a similarity of this complaint with objections raised to the imposition of regulations under the Sarbanes-Oxley Act in the USA as applied to universities and other agencies (e.g., Fischer & Montodon, 2005; Rosenbloom, 2006). If this is the case, then it makes sense to integrate risk management within existing institutional practices.

Conceptually, ISO 31000 provides a more useful roadmap to establish a risk management framework because it looks at the complementarity between risk management and QA and QC processes. Complementarity exists beyond risk management looking at quality practices as methodologies to support part of the process as suggested by Protivity (2007). Harvey and Green's (1993) definition of quality for higher education supports this premise: quality as exceptional, quality as perfection or consistency, quality as fitness of purpose, quality as value for money, quality as transformation. Risk management does provide a different approach toward quality as perfection – think risk tolerance – nonetheless there are more similarities than not on the other points when looked at different levels within a university. Risk management works when integrating all aspects of the internal environment to meet the exigencies of the external environment. The issue at play is coming up with a solution that is not an onerous addendum to existing tasks. The frameworks presented in this paper suggest one approach toward meeting this goal. Under this model, university activity is both evaluated by risk factors and shaped by its identification and management strategy.

References

Argyris, C. & Schön, D.A. (1974). *Theory in practice: Increasing professional effectiveness*. San Francisco: Jossey-Bass.

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

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

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

Birnbaum, R. (July 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

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

Committee of Sponsoring Organizations of the Treadway Commission [COSO]. (January 2011). *Embracing Enterprise Risk Management: Practical approaches for getting started.* Chicago: Author. Retrieved from http://www.coso.org/documents/EmbracingERM-gettingStartedforWebPostingDec110_000.pdf

Committee of Sponsoring Organizations of the Treadway Commission [COSO]. (May 2013). *Internal control – Integrated framework Executive Summary*. Chicago: Author. Retrieved from http://www.coso.org/documents/coso%202013%20icfr%20executive_summary.pdf

Curtis, P. & Carey, M. (2012 October). *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

Del Favero, M. (July 2002). *Faculty – administrator relationships and responsive decisionmaking systems: New frameworks for study*. Paper Presented at the Research Forum on Higher Education Governance June 9-12, 2002, Santa Fé, New Mexico. Retrieved from http://www.usc.edu/dept/chepa/gov/rf2002/delfavero.pdf

Department for Business Innovations & Skills. (June 2011). *Higher education: Students at the heart of the system.* London: Author. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/31384/11-944-higher-education-students-at-heart-of-system.pdf

Dow, K.L. & Braithwaite, V. (2013). *Review of higher education regulation report*. Canberra: Commonwealth of Australia. Retrieved from http://www.innovation.gov.au/highereducation/Policy/HEAssuringQuality/Documents/FinalReviewReport.pdf

Downer, J. (2011). On audits and airplanes: Redundancy and reliability-assessment in high technologies. *Accounting, Organizations and Society, 36(4-5),* 269-283.

Drew, S.A., Kelley, P.C., & Kendrick, T. (2006). Class: Five elements of corporate governance to manage strategic risk. *Business Horizons, 49(2),* 127-138.

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

Fischer, M., & Montodon, L. (Winter 2005). Qualifications, diversity, and workplace practices: An investigation of higher education internal audit departments. *Journal of Public Budgeting, Accounting & Financial Management*, 17(4), 488-521.

Foucault, M. (2008/1978-1979). *The birth of biopolitics: Lectures at the Collège de France 1978-1979*. New York: Picador.

Foucault, M. (1980). Truth and power. In Gordon, C. (Ed.), *Power/Knowledge: Selected interviews and other writings 1972-1977 by Michel Foucault.* (pp. 109-133). New York: Random House, Inc.

Harvey, L., & Green, D. (1993). Assessment & Evaluation in Higher Education. *Assessment & Evaluation in Higher Education*, 18(1), 9-34.

Higher Education Funding Council for England [HEFCE]. (May 2001). *Risk management: A guide to good practice for higher education.* Publication 01/28. London: Author. Retrieved from http://webarchive.nationalarchives.gov.uk/20120118171947/http://www.hefce.ac.uk/pubs/hefce/2001/01_28/01_28.pdf

Jeacle, I. & Carter, C. (2011). In TripAdvisor we trust: Rankings, calculative regimes and abstract systems. *Accounting Organizations and Society, 36*, 293-209.

Juran, J.M. (1999). How to think about quality. In J.M. Juran, A.B. Godfrey, R.E. Hoogstoel, & E.G. Schilling (Eds.), *Juran's Quality Handbook* (2.1-18). (5th ed.). New York: McGraw-Hill.

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.

Landecker, W.S. (1951). Types of integration and their measurement. *American Journal of Sociology, 56(4)*, 332 -340.

Lumann, N. (1994/1984). *Social systems*. Stanford, CA: Stanford University Press.

Miller, P. (2001). Governing by numbers: Why calculative practices matter. *Social Research, 68(2)*, 379-396.

National Association of College and Business Officers [NACUBO]. (2005). *Taking the right path: Sarbanes Summit*. Washington, DC: Author. Retrieved from http://www.nacubo.org/documents/business_topics/SOXsummitfinal.pdf .

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.

O'Donnell, E. (2005). Enterprise risk management: A systems-thinking framework for the event identification phase. *International Journal of Accounting Information Systems, 6(3)*, 177-195.

Porter, M.E. (1996). What is strategy? *Harvard Business Review, (6)*, 4-21.

Power, M. (2007). Business risk auditing – Debating the history of its present. *Accounting, Organizations and Society, 32(4),* 379-382.

Power, M. (2012). The apparatus of fraud. *Accounting, Organizations and Society, http://dx.doi.org/10.1016/j.aos.2012.07.004*

Protivity. (2006). *Guide to Enterprise Risk Management: Frequently asked questions.* Melbourne, AUS: Author. Retrieved from http://www.protivity.com.au

Rhoades, G. (July 2003). *Democracy and capitalism, academic style: Governance in contemporary higher education*. 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/rhoades.pdf

Risk and Insurance Management Society [RIMS]. (2012). *Executive Report: The risk perspective – Exploring risk appetite and risk tolerance*. New York: Author. Retrieved from http://www.rims.org/resources/ERM/Documents/RIMS_Exploring_Risk_Appetite_Risk_Tolerance_0412.pdf

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

Rosenbloom, D.S. (2006). Take it slow: A novel concept in the life of Sarbanes-Oxley. *Washington and Lee Law Review*, 63(3), 1185-1217.

Scarlat, E., Chirita, N., & Bradea, IA. (2012). Indicators and metrics used in the Enterprise Risk Management (ERM). *Economic Computation and Economic Cybernetics Studies and Research, 46(4),* 5-18.

Stufflebeam, D.J. & Shinkfield, A.J. (2007). *Evaluation theory, models, & applications*. San Francisco: Jossey-Bass.

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

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

Westmeyer, P. (1990). *Principles of governance and administration in higher education*. Springfield, IL: Charles C. Thomas Publishers.

Wildavsky, A. (1972). The self-evaluating organization. *Public Administration Review*, September/October, 509-520.

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research, 20,* 69-81.