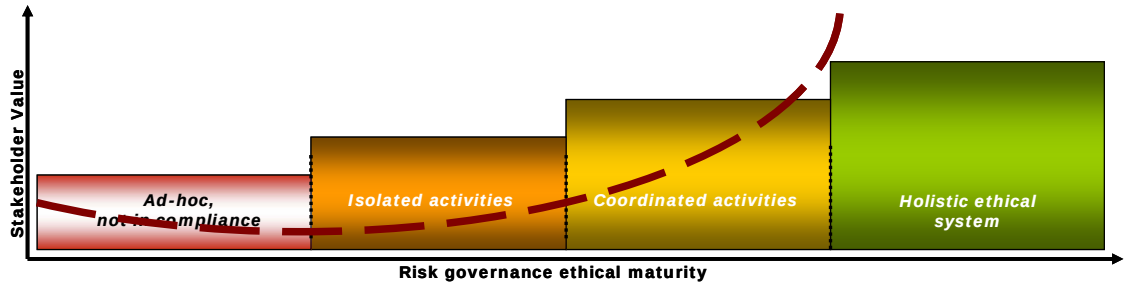
FRAMEWORK FOR AN ETHICAL MATURITY INDEX

Authors: Elena Demidenko and Patrick McNutt

Across key Enterprise risk management frameworks, COSO ERM (http://www.coso.org) and ASNZ4360 (ASNZ 4360: 2004 (http://www.standards.com.au) there is a need to equip organizations with ethical tools which can help them understand how powerful good governance has become in driving the risk management.

Our Framework for an Ethical Maturity of risk governance consists of a maturity scale and criteria. It builds on the work of McNutt (2006) and Demidenko (2006). ERM is positioned as a key enabler of an organisation's ethics, its strategy and performance. It evolves as an intelligent system from which is embedded in the organisational practices of doing business and contributes to the development of an organisation's competitive advantage, and thus maximising shareholder value as illustrated in Figure 1. ERM development implies J-curve principles.

Figure 1: Risk governance ethical maturity scale



A simple governance code can deliver value. This is the essence of the J-curve. Within the J-curve principles, an organisation with a narrow scope of activities, delivering value to a limited number of stakeholders, is positioned on the left of the J-curve. [e.g. private companies with a single owner]. As a company grows the number of stakeholders increases; the company implements some change management initiatives including adoption of governance codes, hence the stakeholders' value may change, and ultimately the value to multiple stakeholders, including the shareholders, increases once the governance matures. As the number of stakeholders increase and as the activities become more complex, a maturity scale may be appropriate as an evaluation-performance tool.

General characteristics of the risk governance maturity ethical objectives are presented in table 1 below.

Table 1 Risk governance ethical maturity objectives

Not in Compliance **Accountability ≠ Responsibility** **No Duties**	**Ethical Compliance** **Accountability = Responsibility** **Duties Fulfilled**		
Lack of RM structure, duties & responsibilities.	Nominal RM structure, duties & responsibilities at the top level.	Consistent RM structure, duties & responsibilities at the top & middle level.	RM roles & responsibilities are aligned to organisational authorities & accountabilities.
RM activities depend on individual initiative and verbal knowledge.	Uncoordinated top down RM activities in some functional units.	Coordinated RM activities enterprise-wide.	RM is embedded in the enterprise management. .
Risk to organisational integrity & ethics.	Risk to organisational integrity & ethics.	Evident organisational integrity & ethics.	Strong integrity & ethics on all levels.

Maturity ethical framework has been structured based on the parameters and components of risk governance (as a foundation of enterprise risk management). The parameters have been derived via analysis of the principles of sound Corporate Governance as well as Internal Environment articulated in COSO ERM. We have taken into account international regulatory requirements to risk governance articulated by London Stock exchange, New York Stock Exchange and Australian Stock Exchange.

Key milestones for risk governance development are the result of analysis of international practical developments and implementation challenges in risk governance.

While risk governance covers broader spectrum of principles, risk governance ethical maturity framework is focused on its key pillars:

- Ethical values
- Duties
- Responsibility and accountability
- Sustainability of risk management: activities / internal controls, sponsorship, commitment to competence
- Transparency

Detailed risk governance ethical maturity criteria are presented in table 2. Each of the maturity levels implies achievement of the criteria for the previous one.

Table 2. Risk governance ethical maturity criteria

Ethical risk governance component	Ad-hoc	Isolated activities	Coordinated activities	Holistic ethical system
	Not in Compliance	**Ethical compliance**		
Ethical values	***Risk to organisational integrity & ethics***	***Risk to organisational integrity & ethics***	***Evident organisational integrity & ethics***	***Strong integrity and ethics***
	- Not articulated / integrity is based on personal trust.	- Documented.	- Documented and consistently demonstrated.	- Inherent to the behaviour on all organisational levels.
Duties	***Duties not fulfilled***	***Duties are defined***	***Duties are fulfilled by senior and middle management***	***Duties completely fulfilled***
	- Responsibility is not equal accountability, or - Lack of accountability for RM	- Nominal responsibility. - Nominal accountability.	- Senior executives and middle management are accountable for any risks taken in line with their risk management responsibilities.	- Accountability is consistent with and inherent to responsibility at all organisational levels, documented in risk policies and job descriptions.
Responsibility and accountability	***Responsibilities are undefined***	***Responsibilities are nominal***	***Responsibilities are consistent across the organisation for senior and middle management***	***Responsibilities are consistent at all organisational levels***
Responsibility	- Responsibilities are not defined. Risks are attended, issues are dealt with based on individual initiative, knowledge.	- Responsibility are formally defined for the Board and senior executives. - Allocation of responsibilities at lower level lacks consistency across organisation.	- Responsibility is defined for risk management in line with risk appetite. - Responsibility for definition of risk appetite lies with the Board and executive directors. - Allocation of responsibility is consistent across organisation	- Responsibility is defined to apply risk management as a value adding activity - Responsibility for risk management is an inherent component of responsibilities on all organisational levels.
Accountability	- Individual accountability for managing of risks / specific	- Accountability of the Board and senior executives relates to	- Accountability is allocated to senior and middle management	- Accountability is integrated with risk appetite, delegation of

Ethical risk governance component	Ad-hoc	Isolated activities	Coordinated activities	Holistic ethical system
	Not in Compliance	**Ethical compliance**		
	groups of risks is not defined. - RM is not a performance measure.	ensure risk assessment is performed and reporting the results of risk assessment in line with compliance / external stakeholders requirements. - Accountability for specific risks taken is not assigned. (Owners of risks are not assigned). - RM is not a performance measure.	for key controls around strategic risks, assurance to executive directors and the Board. - Accountability is assigned for specific strategic risks taken. (Risk owners are assigned to strategic risks.) - RM is a performance measure of the company but of the personal performance. - People are better aligned to manage risks in an effective and efficient manger. Hence, there is more acceptance of risk accountability.	authority, performance management and an organisation value. - RM roles and accountabilities are incorporated in personal objective setting, performance appraisal and reward structures. - Accountability is defined for the Board, its committees, executive directors, management and business functions.
Board and senior executives	- Board operations relating to RM are not defined. - Board audit or risk management committee does not exist / is not involved in oversight of RM activities.	- Board operations in RM are nominal and relate to endorsement of RM compliance. - Board audit or risk management committee is focused on reporting and compliance. - Relationship between the executive and the board for risk and control has not been clearly	- Board operations are clear and documented and reflect the principles of good corporate governance. - Board audit or risk committee displays elements of better practice for committees of this type. - The executive directors have a delegated authority from the board on RM and control	- Board operations reflect leading practice from a corporate governance and compliance RM perspective. - RM structure includes a board committee with RM oversight responsibility, covers a range of functional committees: investments, R&D, quality. - The RM authority of executive directors given by the Board is

Ethical risk governance component	Ad-hoc	Isolated activities	Coordinated activities	Holistic ethical system
	Not in Compliance	**Ethical compliance**		
		articulated. - Board and executive agendas do not include risk and control as a core matter.	- Board and executive directors agendas include risk and risk mitigating actions as a separate matter	practical for managing business and in line with DOA. - Board and executive directors agendas include challenge to the RM, understanding of risks or risk reviews to make better strategic decisions and enhance stakeholder value.
Sustainability of risk management	***Sustainability depends on individual initiative / a single trusted person / owner***	***Low sustainability***	***Sustainable activities in management of strategic risks***	***Sustainability is assured by strong integrity and ethics on all level.***
Internal controls / activities	- Risk management is not a "tone at the top" - No review of performance / compliance with the risk management policy. - Ad-hoc RM activities of the Board / functional leaders are based on individual initiative and personal knowledge.	- RM policy , strategy is driven centrally entirely from the top. - Some risk management activities occur in functional units. - Internal review of compliance with the RM policy and procedures (internal compliance check-list). - Board Committees are reviewed against their charters.	- Elements of "bottom up" approach to setting of the RM strategy. - Risk management activities coordination is ensured via some elements of matrix risk management structure. - Internal audit and independent review are primary mechanisms to maintain accountability and commitment to good RM. - Risk and audit committees can enforce accountability for sustainable risk management. - A corporate ERM function helps to develop and drive risk policies and a framework.	- Business units are formally engaged in setting the RM strategy and in linking this to the business strategy - Risk management activities are integrated and coordinated enterprise-wide, embedded in the way of doing business - Board, audit committee, senior executives, internal audit review risk management activities in order to maintain accountabilities. - Board committees are reviewed and monitored against their charters and improvement plans are in place.

Ethical risk governance component	Ad-hoc	Isolated activities	Coordinated activities	Holistic ethical system
	Not in Compliance	**Ethical compliance**		
			- Risk manager / Chief Risk Officer acts as risk management process facilitator / internal consultant to executives and produces consolidated risk profile to the Board. - Risk management KPIs are determined for the key participants of the process based on the risk management objectives. .	- Chief risk officer fulfils his / her duties being accountable for management of the organisational risk profile. - A corporate ERM function's focus and scope move from process to more value-added insight and analysis. Risk executive monitors and helps with new RM techniques, training, oversight and insight. - Risk management KPIs are monitored and are base for reward and recognition in the performance management process.
Risk management structure	- Lack of risk management structure.	- Senior executives are key owners of the risks of their functional units. - Lack of coordination of risk management activities relating to the same risk (inefficiency of functional silos). - Internal audit owns the corporate process of risk assessment to focus the internal audit plan and foster	- Ownership of the business risks is embedded in the business units, while ownership of the risk management process is allocated on the corporate level. - Corporate ERM function drives ERM and coordinates of risk management activities relating to the same risk exist across the functions.	- Risk management structure is effective for the strategic and operational risks. - Risk management process is integrated on the corporate and business unit levels. - Risk owners have matrix reporting line aligned to business value drivers across functional silos, i.e. is aligned to an organisation's value map,

Ethical risk governance component	Ad-hoc	Isolated activities	Coordinated activities	Holistic ethical system
	Not in Compliance	**Ethical compliance**		
		compliance. - Initial risk champion resides with internal audit, has direct access to the audit committee and facilitates entity-wide risk inventory development for compliance purposes, but not tools to manage the risks it measures. - Internal audit is not a review mechanism for ERM process /system.	- Risk owners and mitigating action owners are assigned for key risks. - Risk champion resides within one of the functions: legal, treasury, strategic planning, internal audit and provides internal consulting to manage entity-wide risks. - Internal audit acts as part of ERM system and is accountable for monitoring the effectiveness of risk mitigating actions, and for independent review of ERM process.	addresses business diversification and effective to overcome inefficiency of functional silos [1]. - ERM function is imbedded into functions / business units. Risk executives with deep industry / business knowledge are either in the central ERM function or in a allied area: strategic planning, finance, legal, treasury.

[1] Risk owners are assigned to each of the strategic risk category or key risk area (value driver). Business unit's risks are aggregated based on the key risk areas by Senior Executives and reported to the Owner of relevant key risk area. Such a structure will greatly assist in enhancing transparency and consistency of risk management in the diversified business where importance of effective "cross functional" risks management will be higher. It will also enable an organisation to streamline achievement of objectives in each of the business value drivers.

Ethical risk governance component	Ad-hoc	Isolated activities	Coordinated activities	Holistic ethical system
	Not in Compliance	**Ethical compliance**		
Sponsorship	- Lack of top-down sponsorship of RM in the organisation.	- Limited "top-down" sponsorship by the Board and audit committee is aimed to ensure sustainability of risk assessment reporting and compliance. - Leaders of functions / business units are forced to sponsor risk assessment to comply with internal / external regulations. - Lack of proactive sponsorship by the CEO.	- Sponsorship penetrates from the "top down" to functional / business units and reinforced by the accountability of senior executives and middle management. - The CEO has direct input into the sponsorship process. - Champions / sponsors are identified across the organisation.	- Strong tone at the top and leadership for RM across the organisation. - Senior executives set RM objectives for their own functional / business areas. - Strong bottom up support. RM is naturally accepted across the organisation.
Commitment to competence	- RM skills are not developed, supported nor assessed.	- Limited appreciation of the skills in RM within organisation.	- Board, audit committee and senior executives are committed to competence. - Skills of the Board and its committees are reviewed and upgraded. - Systemic approach to develop competence of personnel so that they are proficient to achieve organisational goals.	- Entity-wide commitment to competence is part of organisational culture. - Board / audit committee, executive and personnel are capable to manage risks as part of business operations. - Formal RM training to participants of the process or all personnel.
Transparency	***No transparency or coordination of RM activities across the business***	***Low transparency. Limited coordination of RM activities between functions***	***Some transparency. Coordinated RM activities across functions***	***High transparency. Formal RM structure consistently embedded across all organisational areas***

Ethical risk governance component	Ad-hoc	Isolated activities	Coordinated activities	Holistic ethical system
	Not in Compliance	**Ethical compliance**		
				including strategic planning, capital allocation, product development, etc
Risk management communication	- No guidance on risk management activities. - Risks management mission statement , policy and strategy are not developed. - No evidence of communication from the top on RM.	- Risk management mission statement and general policy developed for compliance and communicated to the board. - Key risks are disclosed to external stakeholders to fulfil compliance requirements (e.g. SEC, form 10-K) - Some communication from the top to provide a fairly consistent view of why the company needs RM. - Risk vocabulary is articulated in the risk management policy	- Risk management mission statement and policy define the purpose, ultimate value of ERM and its ultimate scope. - Risk management policies are developed for key risk categories and tie to business objectives. - Responsibility to manage specific risks along with accountability for any risks taken is a major component of any risk policy. - Communication from the top is clear. - Management's philosophy and operating style supporting risk awareness and consistently promote the need for good RM throughout the entity. - Common risk vocabulary is aligned and compatible with the company's language, value drivers and culture.	- Risk management mission statement, strategy and policy are embedded in the way of doing business. - ERM is integrated with the stakeholders communication. - Internal & external communication on RM is consistent. Risk policies and practices to the board and external stakeholders (e.g investors, suppliers, and rating agencies). - Strong consistent communication of the importance of good RM, including benchmarking to position the company in the context of its peers.

Ethical risk governance component	Ad-hoc	Isolated activities	Coordinated activities	Holistic ethical system
	Not in Compliance	**Ethical compliance**		
Clarity of risk management process and structure	- No guidance on risk management activities. - RM structure is undefined.	- High level risk policy substitutes risk management methodology and process. - RM structure is implied in high level accountabilities of the Board, committees, senior executives and a corporate ERM function. - The role of support business functions (legal, HR, etc) in the RM structure has not been defined - No consistency in structure across all business areas.	- Clear and formal risk management process is well documented in the policies. - Risk owners and risk management process participants are identified and acknowledged. - RM structure is clear and aligned to business objectives. - The role of support business functions is articulated through the internal control procedures and policy. - Consistency in structure for management of company level risks, some duplication / inconsistency exists.	- Risk owners understand, acknowledge and fulfil their responsibilities in the way of doing business. - Support business functions are incorporated into the RM structure, set policy and monitor compliance. - RM organisational structure clearly aligns all parts of the business, supports single view of RM approach.