



## **BridgeWork : an effective approach to transition from risk assessment to Enterprise Risk Management using ISO3100**

## Where Does Enterprise Risk Assessment (ERA) Lead Your Organization?

For many organizations, a risk and control self assessment (RCSA) is considered the best way to gather information about risk profile, control environment, processes, training and awareness, ethics and compliance programs, segregation of duties, monitoring activities and more.

These types of self assessments, along with interviews or consultations, are often used to canvas senior management, subject matter experts, and areas with unusual operations, to assess the level of risk and to evaluate the controls in place. Voting or polling techniques are also often used to facilitate workshops, where multiple answers are weighted and aggregated to gain insight into various risk profiles.

Self assessment and voting tools have proven to be very useful and have allowed managers to forge greater collaboration between functions, peers, management and operations, as well as measuring certain “soft” (qualitative) controls that cannot be quantified, calculated or verified otherwise. There are, however, substantial limitations in these tools when applied to enterprise risk management.

## Assessments Can Have Limited Value

The results of a self assessment, an interview or a voting workshop can frequently be found to be of limited value due to several factors. For example, characteristics of the participants, such as their perspective, their level of maturity, and their understanding and experience as it pertains to risk management, cannot be assumed to be thorough or uniform unless significant context is provided beforehand which, in our experience, seldom occurs. Consequently, the RCSA may not produce enough meaningful information and insight into the actual risk profile to enable development of a comprehensive action plan in line with the risk appetite of the organization. Additionally, because most risk events occur in operations, the risk response and action plans become challenging for the risk management team, who often find it difficult to coordinate centrally.

The limitations of these techniques lead organizations that depend on them for effective risk management down a path that is characterized by incomplete or misleading information, inefficient deployment of resources, and poorly coordinated and ineffective risk treatment plans. It becomes difficult to measure performance or to use risk management to attain the organization’s objectives.

## Proven Global Standards: ANZ 4360 and ISO 31000

When looking at examples of best practice, the Australia/New Zealand Standard 4360, or AS/NZS 4360 stands clear above all others. Implemented across thousands of organizations in dozens of countries, and continually refined over a number of years, this Standard has shown resilience as a practical, value generating risk management framework that encourages sound management principles.

The recently ratified successor to the AS/NZS 4360 Standard is the global ISO31000 Standard which is in most part based on the AS/NZS Standard. The ISO31000 Risk Management Standard, presents an opportunity to mature the risk management processes in organizations and move organizations to a higher level of ERM maturity. ISO31000

## BRIDGING THE GAP BETWEEN ERA AND ERM WITH ISO31000

encourages broad organizational participation driven by a common risk management methodology, vocabulary and blueprint for excellence. If risk management is everyone's job, ISO31000 facilitates that democracy.

Cura has abstracted some key lessons from ISO31000 companies in formulating BridgeWork, a set of services, advisory and solutions that assist organizations to achieve more mature risk management programs.

### **The “Bridge” that Leads the Organization to Effective Risk Management**

As described above, organizations understandably experience difficulty attaining maturity in risk management. Often what passes for enterprise risk management is usually periodic assessment of historical data that fails to deliver lasting value. Organizations are further hampered by intricate and conflicting theoretical literature, frameworks and standards promoted by a myriad of interest groups.

In light of these findings, it is easy to understand why many organizations have not moved very far along the risk management maturity curve. Instead, the focus has remained on Enterprise Risk Assessment for governance and reporting purposes. This report-focused environment encourages a silo based approach to risk management, wasting untold time and money and resources in complex, isolated, redundant activities, failing to unlock the value of ERM.

Fortunately, the "bridge" that will lead organizations from traditional Enterprise Risk Assessment (ERA) to Enterprise Risk Management (ERM) is very well defined in the ISO31000 Standard, summarized in its "Attributes of Excellence in Risk Management" section (outlined below), and is worth consideration when formulating a risk management program.

## ISO31000: Attributes of Excellence in Risk Management

The ISO31000 risk standard outlines some key attributes that identify excellence in risk management:

1. **A pronounced emphasis on continual improvement in risk management** through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capabilities and skills.
2. **Comprehensive, fully defined and fully accepted accountability** for risks, risk controls and risk treatment tasks. Designated individuals fully accept, are appropriately skilled, and have adequate resources to check risk controls, monitor risks, improve risk controls and communicate effectively about risks and their management to internal and external stakeholders.
3. **All decision making within the organization**, whatever the level of importance and significance, **involves the explicit consideration of risks and the application of risk management** to some appropriate degree.
4. **Continual communications** with highly visible, comprehensive and frequent internal and external reporting of risk management performance to all stakeholders as part of a governance process.
5. **Risk management is viewed as central to the organization's management processes** so that risks are considered in terms of effect of uncertainty on objectives. The organization's governance structure and process are founded on the management of risk. Effective risk management is regarded by managers as essential for the achievement of the organization's objectives. (source: ISO 31000 Draft Standard, 2008)

These Attributes of Excellence form the basis of the Cura Risk Management Methodology. It should be noted, however, that any Methodology or Standard – even multiple ones - can be harmoniously modeled and aggregated using Cura's solutions, while leveraging the positive attributes of ISO 31000. In other words, the productive efforts already underway in client organizations deserve to first be leveraged to their maximum extent as part of the process of discovering whether broad adoption of a unifying framework is appropriate.

## Cura's Five Tactical Themes

Cura has translated the ISO31000 attributes of excellence in risk management described above into five tactical themes that include tools, techniques, reports and methodologies which form the foundation of our ERM solutions and our supportive integrated GRC (Governance, Risk, Compliance) management platform:

1. Enforce accountability
2. Embed risk management
3. Link risk management to strategic decision making, linking risks to both objectives and management actions
4. Communicate widely using reports, events and notifications
5. Manage individual performance by monitoring tasks, measuring maturity, "shame and fame" reports

These five tactical themes are explained in greater detail below.

### **Tactical Theme 1: Enforce Accountability**

Appoint risk champions who will facilitate the risk management process within a business unit region or other significant entity. The role of the risk champion is not to do the risk assessment, nor should the risk champion define or execute the risk treatment and action plans. Schedule regular workshops for all the significant entities of the organization where risk officers from each significant functional area or key organizational driver should participate.

Workshops determine the key risk issues of the organization. Prior to the workshop, the risk champion prepares a short list of generic risk issues or risk events that are known in the organization. The objective of the workshop is to get people talking and discussing the issues rather than focusing on the assessment. It is important that participants understand the need for transparency and accountability and that they accept responsibility for issues that arise.

Here are some points to consider that will help to enforce accountability:

- Focus on risk control effectiveness (RCE) as an essential measure
- Do not recruit new people for risk management; use your own resources
- Set the context for risk management upfront
- Allocate individuals to the risk events (not functions)
- Associate the strategic plan or organizational objectives to the risk profile
- Set reasonable deadlines to update the risk registers with existing or proposed action plans
- Use the risk committee and governance structure to drive accountability
- Use management information systems to monitor risk and action progress

### **Tactical Theme 2: Embed Risk Management**

A regular, defined reporting period helps to engage the risk officers and to gain traction. Ideally, the deadlines for the rollout of the ERM process should coincide with the reporting period for the first 2-3 periods. Managers use the information that is reported at the risk management meetings to manage their own activities. Those activities may be delegated to, or closely involve input from, persons close to the impact or root cause of the risk event.

Risk management should be embedded in the business processes throughout the organizational hierarchy of accountability and progress of all action plans and risk treatment should be tracked and reported against the risk register.

## BRIDGING THE GAP BETWEEN ERA AND ERM WITH ISO31000

The periodic risk management meeting is a forum for discussing all updates to the risk registers that were performed by the risk officers. Emphasis should be placed on any risks that should not be tolerated because they exceed the risk appetite of the organization. The risk response and risk treatment plans for those risks that do not match the organization's appetite should then be reviewed and adjustments planned.

- Create simple risk "watch-lists" that management can use in meetings
- Link risk management to decision making within each business unit
- Start with the business process maps
- The risk management process rolls down and outward into the organization; risk events then roll up
- Use the risk management processes: Root Cause Analysis, Control Assurance, and Risk Assessment.

### Tactical Theme 3: Link Risk Management to Strategic Decision Making

The risk assessment and management process should be invoked whenever decisions need to be taken on significant investments, capital projects, strategic plans, legal or regulatory changes, new initiatives, organizational drivers or any other uncertainty that the organization encounters.

It is important to set the context for risk management in the organization upfront. Whether it is to improve efficiency, reducing incidents, establishing a healthy and safe work environment, protecting shareholder value, the environment or the employees, drive strategic product development or maximizing opportunity in uncertain times, the information collected during the risk management process can be used to measure the of the objectives that the organization has defined.

Define the internal and external context up front. Once the executive risk assessment is completed, communicate the context for risk management widely and use this to drive the risk management process down the organizational hierarchy. All risk events should then be rolled up iteratively to the significant entities during the quarterly risk workshops.

Define risk issues using short definitions that span multiple entities. Each risk issue is described as a possible event in the context of the entity where it occurs. By using short definitions, risk issues can easily be rolled within and across entities. Risk issues are assessed in each of the entities within the organization by documenting the effect that uncertainty has on the particular entity. Once the assessment is completed and risk treatment plans are in place, the risk owners can then specify target risk ratings that will demonstrate a "gap" that equals the organization's risk tolerance for the assessment period. These "cross cutting" risks can then be reported across the significant entities by indicating the level of risk above the risk appetite set for the organization. This is a valuable oversight tool for helping senior management to allocate resources more effectively. Points to consider:

- No risk assessment = No approval - and there should be no exceptions!
- Do not make decisions primarily on monetary values
- Think about "Liability" and "Potential Exposure" but also consider possible "Opportunity" in uncertainty
- Link to the delegation of authority system - use risk assessment and its rigor
- Use total exposure assessment to prioritize assurance activities

## Tactical Theme 4: Communicate Risk Management Widely

All risk management, risk treatment and action plans deserve wide communication and organizational involvement. This communication includes the context of risk management, risk framework and intentions, as well as the risk management plan. Every risk, control and action item in the system must have an owner who is both accountable and empowered to manage that risk.

Risk registers are best kept consistent so that changes can be tracked over time. Post-workshop, participants obtain and create reports to assist them in further assessment, analysis, investigation and planning, and to capture the necessary details. Risk officers delegate action to resources within their functional areas, and management meetings become the forum to communicate risk treatment plans to those responsible parties. Tasks are assigned to task owners, and progress is tracked to ensure effective risk management.

The organization will only get full value from reporting if it includes employees, management, risk management committees, audit committees, stakeholders and shareholders.

When reporting, rather than focusing on what the risks and risk ratings are, consider reporting rather on:

- How fast is our risk management improving?
- How well are we managing the risk profile?
- What are the challenges in our risk profile?
- Why are these challenges there?
- How can we improve our process to address the challenges?
- What are the emerging risks?

## Tactical Theme 5: Measure Performance in Risk Management

Because the management of risk directly affects organizational objectives, business units and individuals are held accountable for timely risk treatment and action plans. This helps to drive accountability and ensures that risk exposure is managed within the risk appetite of the organization. Action items are implemented according to established schedules and monitored regularly to ensure that the risk management process is effectively maximizing opportunities and reducing the impact or probability of loss as well as protect and increase shareholder value. Risk management is thus tied to organizational performance and governance.

It is thus recommended that one develops tools to measure performance such as Key Performance Indicators (KPI's) for business and personal management improvement. KPI's can be based on the risk management plan by setting reasonable targets for business units and individuals and be driven by risk maturity tools and assessments. Linking risk management to performance management to encourage effective and sustainable risk management

## BRIDGING THE GAP BETWEEN ERA AND ERM WITH ISO31000

Examples of KPI's could include:

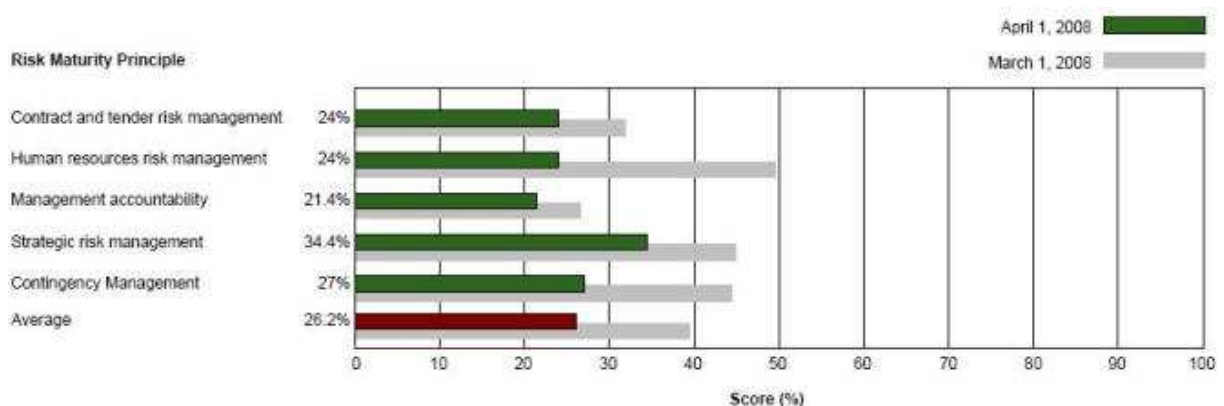
- Proportion of treatment tasks for high risks completed this month
- % progress made with risk management plan
- % annual change in risk management maturity evaluation score
- % change in exposure above risk appetite
- Reward innovation in process and control improvement and efficiency or cost savings

### An Example of a Risk Maturity Program

Cura recommends that an evaluation be conducted to determine the context for risk management in the organization, the level of understanding and experience in the team, and the governance structure in place. From the Risk Maturity Evaluation, a Risk Maturity Program will be developed. The risk maturity program is the first step to drive management accountability for risk management and generate the Risk Management plan. The level of maturity for risk management is monitored and reviewed periodically.

Risk maturity programs are a set of principles or elements that should be aligned with the strategic plans, culture and practices of the organization. The program is reviewed, improved or changed at any time and is used to drive or change the focus of risk management, the context of the risk management program, or to "raise the bar" of the business practices of the organization.

Division	Healthcare	Engines	Finance	Media
Ave Maturity	13.2%	35.4%	52%	38.1%
Key Gaps	- Strategic Risk Management - Contingency Management	- Contingency Management - Contract Risk Management	- Credit Risk Management	- Human Resource Risk Management



## Conclusion

Organizations in search of a sound set of frameworks and principles for developing a resilient, risk-aware, opportunistic culture can find guidance among the world's best examples of Enterprise Risk Management. Our own research has pointed repeatedly at ISO31000 as a key driver for success in ERM.

After having completed over 250 broad ERM deployments in some of the most complex, heavily regulated companies in the world, Cura has distilled the Five Tactics outlined in this paper and made them available to assist organizations in ramping up their ERM efforts successfully.

Experience has shown that these Five Tactics represent essential underpinnings of a transformative ERM program that is within reach of any size organization in any industry. Adherence to the principles contained within these Five Tactics is a sound step toward bridging the gap between Enterprise Risk Assessment and Enterprise Risk Management and attaining greater benefit from an ERM program.

## About BridgeWork

BridgeWork, is an advisory service from Cura coupled to Cura's best practices ERM solutions. It is the natural result of numerous successful client implementations. Cura offers this capability to organizations intent on attaining the benefits of a resilient ERM culture.

The standards-based principles and experience that form the BridgeWork service also form Cura's product and technology road map, assuring clients of a cohesive, best in class suite of tools, techniques and product solutions.

Cura BridgeWork provides the enabling technology, best practice and experience that any organization can use as a guide to integrate any of the governance risk and compliance processes

## About Cura Software

Cura Software Solutions enables businesses around the world to quickly achieve the bottom line benefits of enterprise-wide governance, risk management and compliance (GRC), coupled with performance management. Cura does this through fast implementation, easier configurability and true enterprise architecture.

Cura is used by over 250 customers such as BHP Billiton plc, Westfield, Allianz, Old Mutual plc, GlaxoSmithKline, Standard Bank, Virgin Blue, Vodacom, as well as governments and consulting firms world-wide.

Cura has offices in New York, Boston, London, Sydney, Melbourne, Johannesburg, Singapore and Hyderabad and has distributors in 10 countries (South America, Middle East and Asia). Cura is a wholly owned subsidiary of SoftPro Systems Limited (NSE/BSE:SOFTPRO).

For more information, visit <http://www.CuraSoftware.com>.