WHITE PAPER

# 8 Principles of Risk Convergence and Implications for GRC Technology Solutions

MAY 2008

OpenPages

Clarity. Confidence. Control.

## Table of Contents

## Executive Overview

Security breaches involving customer records and multi-billion dollar losses arising from rogue trading activities are just some of the high profile risk events that amplify the critical importance of Governance, Risk and Compliance (GRC) to a firm's economic health. Meanwhile, the reverberations of the subprime crisis have dramatically affirmed the interdependence of varied risks across an enterprise, which need to be managed holistically rather than in traditional silos.

Managing risk and compliance in silos is both cumbersome and costly. For each new regulation or risk discipline, organizations typically implement a new technology point-solution. This fragmented approach limits an organization's ability to streamline risk and compliance processes and reduce costs. It also obscures the opportunity to integrate risk and compliance to gain a holistic view of the firm's risk landscape.

Not surprisingly, the frequency of risk events that create negative headlines and the inefficiency and ineffectiveness of a siloed approach is generating renewed interest in the convergence of GRC within the firm. A recent Ernst & Young study showed that convergence is under way at a large number of organizations. Yet the survey also underscored that although risk convergence is in progress there are no agreed upon best practices. When it comes to risk convergence, firms are for the most part still on the lower half of the learning curve.

There is confusion about the benefits of GRC convergence because the industry uses enterprise risk management (ERM) and risk convergence interchangeably. ERM attempts to integrate risk disciplines, such as operational, compliance, strategic, and technology, to achieve a holistic view of risk exposure across the enterprise. This enhances the visibility into the firm's risk landscape which enables improved, risk-informed business decisions.

Risk convergence, on the other hand, addresses inefficiencies and opportunities within the ERM framework to maximize the cost benefit of conducting risk management processes. The primary goal is to achieve practical process improvement that results in efficiencies and cost saving.

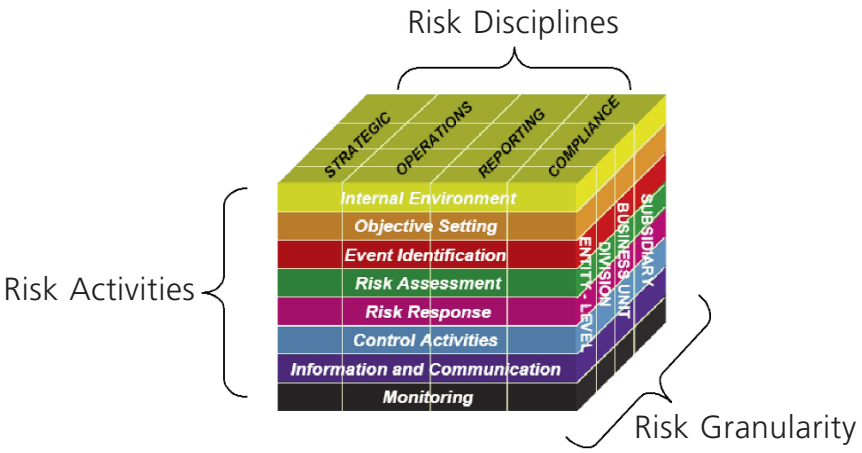
Convergence within a GRC framework is aimed at achieving both ERM and risk convergence objectives. It aids the risk organization in reaching the next level – controlling costs, achieving efficiencies, managing risk and providing better support for business decision-making.

## What Needs to be Converged

The COSO II ERM Framework shown in Figure 1, illustrates the key dimensions of risk convergence: risk disciplines, GRC processes, and risk granularity. The risk disciplines (columns) in the COSO model include strategic risk, operational risk, reporting risk (e.g. financial controls such as SOX), and compliance risk. Depending on your firm's industry and specific objectives for GRC, you may add additional disciplines such as market risk, credit risk and technology risk.

Whatever risk disciplines are significant within your firm, the goal is to integrate them within a single framework that produces a holistic view of your risk landscape. However, many technology solutions focus on a single risk discipline, such as operational risk or compliance; these solutions may be appropriate for a siloed approach but they usually lack critical capabilities that are required for GRC convergence.

**Figure 1:** COSO II ERM Framework




The rows in the COSO cube represent the different risk and compliance processes that are involved in an integrated GRC framework. The objective is to integrate activities both across columns and across rows. For example, you would not want to have one system for managing risk assessments for operational risk and a different system for compliance, or different systems for handling loss events separate from risk assessments.

The third dimension in the COSO model—risk granularity—is extremely important for operationalizing an integrated GRC framework. In the COSO cube you see four levels of the business entity structure depicted, however, in practice, there may be any number of levels in the entity hierarchy. There are other hierarchies, such as processes and accounts, which are also very important to represent within your GRC framework.

The level of granularity that GRC processes, such as risk assessment and risk measurement, are carried out will be different across risk disciplines. For example, strategic risk will tend to be conducted at a relatively high level, while SOX will be carried out at a much lower level of granularity, especially in terms of processes, risks, and controls. It is important for your technology solution to have the flexibility to support the right level of granularity for the different risk disciplines and the right level for your organization.

## Principles of GRC Convergence

Now that we have discussed what needs to be converged, we will look at the key principles/requirements of GRC convergence and the implication for technology support.

**Principle 1: Resist "one size fits all" approach**

GRC, similar to most business functions, is not a "one-size-fits-all" solution. It has to be tailored adapted for each firm. As Mark Olson of the Federal Reserve notes:

> "An effective enterprise-wide compliance-risk management program is flexible to respond to change and it is tailored to an organization's corporate strategies, business activities and external environment."

While most leading companies have tailored their risk methodologies to match their business operations, it is imperative to select a technology solution that can easily adapt to your firm's unique risk and compliance methodology and evolve gracefully over time.

The ability to adapt the technology solution to your company's specific risk management methodology and framework, without having to write custom code, is called configuration. The key business benefits of configuration include:

- **Lower costs:** Custom code is more expensive to develop for initial implementation and much more expensive to maintain and extend over time.
- **Time to deployment:** Configuration can support rapid implementation at a fraction of the time compared with writing custom code.
- **Future proofing:** Configuration will allow you to quickly adapt your risk framework to meet changing requirements while minimizing the impact on your business operations.

The extent to which your technology platform is configurable is arguably the most important decision criterion for selecting a solution.

**Principle 2: Convergence should enable you to "Assess once and satisfy many"**

The GRC framework should provide a consistent approach across your organization's businesses by establishing minimum standards for risk management. This will ensure that risk policies, principles and procedures are adequate and effective. By eliminating risk and compliance management silos and harmonizing risk and compliance activities you can greatly reduce the burden on the business lines, avoid "assessment fatigue" and free up resources to focus on achieving goals.

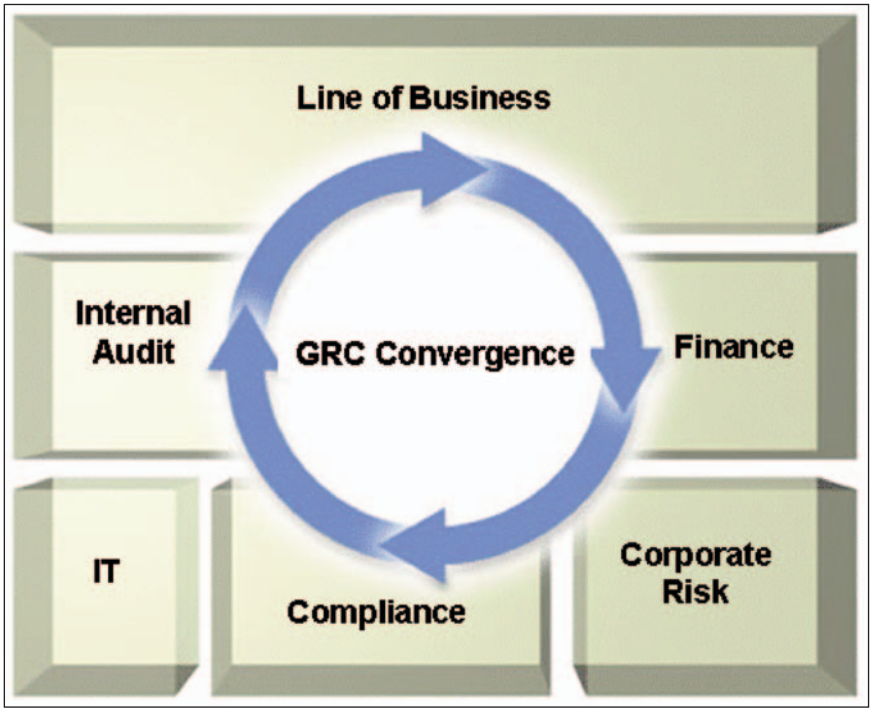
Your technology solution plays a critical role in the effort to converge and harmonize methodology and processes. The technology solution serves as a common repository for all GRC elements including frameworks, risk and control libraries, policies and procedures, and other elements of your risk rating methodology. By implementing a single assessment and sign-off process you can eliminate duplicated and redundant activities.

To achieve a holistic view of risk across the business your firm will need to establish a "common language" for risk activities, which involves creating a rating methodology for all risk data, such as loss events, risk assessments, and key risk indicators (KRIs). The technology solution can help enforce consistency by supporting GRC libraries, risk categorization, calculated fields (for example computing risk rating based on likelihood and severity) and field data validation (for example enforcing that certain fields are required to be filled in for operational risks, and different fields are required for compliance risks). The common language will be specific to your firm so configurability is a critical capability for supporting this principle.

**Principle 3: Convergence requires collaboration and coordination**

A comprehensive approach to managing risk enables organizations to reduce duplication of effort, increase efficiency, and make smarter business decisions. This comprehensive approach requires integrating risk and compliance management processes across the different functional and business groups. The key players are shown in figure 2.

**Figure 2:** GRC Stakeholders




Accommodating the sometime conflicting requirements of these different constituencies is critical to a successful implementation. Different functions within a company will want to tailor risk practices to match their business need. For example, to support SOX requirements, Finance and Audit may conduct very detailed, qualitative risk and control self assessments (RCSAs) for financial processes. Operational risk, on the other hand, may want to perform higher level quantitative RCSAs for key business processes across the enterprise.

The technology solution should enable the unification of your GRC initiatives within a single enterprise system. Through a single system of record and a set of platform services, you will be able to coordinate multiple risk disciplines, allowing functional groups and business lines to efficiently manage integrated risk and compliance processes throughout the business.

Through configuration, your technology solution should enable you to provide each of the different functions their own specific views of key GRC elements such as risk, controls, and assessments. The goal is to leverage what is common but for allow for differences where they are required.

Workflow is a critical factor in helping to coordinate the activities of the difference functions. Workflows should be easy to configure to support the different GRC processes of each function. Workflow can also help synchronize activities across functions; for example, enabling the operational risk (ORM) function to leverage RCSAs performed by the SOX team. Workflows should automate the scheduling of tasks and help to ensure consistency across different functions.

**Principle 4: Convergence requires a cultural change**

The Ernst & Young survey states that people issues are the primary barrier to convergence. For many people, convergence becomes a "turf battle." Others view convergence as a distraction that can dilute their efforts. Many view it as a significant challenge that will demand resources.

Successful GRC convergence requires a culture change that is driven by leadership from the top, and technology can be an important lever. Some of the key goals for cultural change should include:

- Making risk management a part of everyday business activities
- Empowering people by making everyone in the company a risk manager
- Providing risk information that is actionable

Risk management should be viewed as a competency that is embedded in the organization and incorporated in everyday processes at all levels of the organization to produce a competitive advantage. Senior management must make the program a high priority initiative throughout the company and foster a culture that emphasizes the central importance of ethical behavior, quality control, and risk management.

Technology can assist the transition and can be the rallying point that helps promote risk awareness and allows you to institute a supportive risk culture within the organization. Automated risk processes can help to build accountability and distribute GRC ownership into lower levels of the organization. Your technology solution can facilitate training and awareness and help to engage business users by providing actionable information that provides better visibility into their risk landscape.

**Principle 5: Risk management must be actionable**

A common mistake for many risk convergence efforts is to focus too much attention on supporting the requirements of senior management (for example dashboard reports), while neglecting the needs of people in the business who are the first line of defense for risk management.

Your technology solution should play an important role in helping to make risk management actionable. Key requirements include:

- Making the solution easier to use for different, sometime infrequent, users
- Presenting relevant data to the user (rather than forcing them to seek it out)
- Ensuring consistency across GRC processes
- Exciting and empowering users, as opposed to frustrating and confusing them

A great way to bring relevant data to the user is to have a home page that can be easily tailored for different types of users. For example, control testers should have a list of controls that need their attention and assessment reviewers should see the assessments that they need to perform. All users should have issues and action items on their home page so they know what remediation efforts require their attention.

Configurable workflow enables the automation of GRC processes such as review and approval of RCSAs, and root cause analysis for loss events. Your technology solution should be able to:

- Route risk and compliance activities to the right people at the right time
- Monitor risk and compliance activities and track subsequent actions
- Establish triggers and points of escalation so that responsible managers are notified and aware when action is required
- Notify managers when identified action is not taken

The technology solution can be a great aid to the user if it can easily pull together the right data into a single view that supports the activity being performed. The alternative is that the user has to navigate through the system to find the relevant data, and for infrequent users this can be a daunting task.

GRC information should be communicated up, down and across the organization, so reporting is a critical component for making risk data actionable. To support analysis, decision making and action, reporting needs to be timely, accurate and flexible. The presentation of data is important and should include graphs, charts, trends and dashboards.

**Principle 6: Assume risk is everywhere and make it the focal point**

Risk is everywhere in the organization. There is risk to business objectives, risk to processes, risk to new products, risk of non-compliance to regulations, third-party supplier risk, and so on. To adequately understand risk within multiple disciplines you need to be able to assess risk to multiple GRC elements.

For example, for strategic risk assessments you will want to perform high-level, top-down risk assessments at some level in your business entity hierarchy. If you are performing a financial controls assessment you may be concerned with risks to material accounts. You may be focused on risk to key business processes, or if in the compliance group you want to understand risk exposure relative to the regulations that affect your business.

Your technology solution must be flexible, and through configuration, allow you to assess and associate risk to multiple GRC elements. Questions you should ask include:

- Does the solution force a single view of risk; for example, is it process-centric in that it associates risk only to processes?
- Can risk be associated to multiple GRC elements such as entities, processes, policies, accounts and regulations?
- Can risk be categorized at multiple levels using multiple taxonomies, for example Basel II (3 levels), COSO, or your own categorization scheme?
- Can risk be assessed at the different levels of granularity, for example multiple levels in the business entity or process hierarchy?
- Can losses be linked to risks to determine how risk exposure is trending versus actual losses?

**Principle 7: Risk convergence is evolutionary not revolutionary**

Your risk and compliance methodologies will change over time as your GRC framework evolves and best practices mature. In addition, your organization will change due to reorganizations, mergers, acquisitions and divestitures. Your technology solution must be able to evolve with you. The technology solution should enable you to easily modify the GRC elements that you store in the system. For example:

- Configure fields without coding – add fields, remove fields, change their labels, change validation criteria, and so on
- Add new types of information – such as a new requirement to assess risk against third party vendors
- Add new relationships between data elements – for example, you may be tracking losses against the businesses that caused the loss, but now need to also associate losses to the businesses that were impacted by the loss

If your technology solution is rigid and requires software code changes to accomplish the above list, your chances for a long term successful GRC framework will be greatly reduced.

You should expect to evolve your best practices and change your risk management methodology over time. If your technology solution cannot respond quickly to changes in best practices or changes in your business, you will end up with a solution that does not reflect the realities of your business practices and does not meet the requirements of your users.

**Principle 8: Make business process management a priority**

Good risk management is a natural outcome of good process management. An organization with well-managed business processes will be less subject to breakdowns, errors, and other forms of GRC risk. So focusing on improving business processes will result in less errors and losses.

Implementing business process management (BPM) standards is conceptually simple, but requires investment of time and attention. BPM is a relatively mature discipline, with proven tools to ensure effective management and control, but it requires an appropriate degree of rigor in the design and management of your business processes. The key elements to focus on include:

- Clear accountabilities
- Process objectives/requirements
- Control design and improvement
- Monitoring and measurement

The first step in implementing BPM is for each major division to establish their "process hierarchy" and identify their "critical" processes. The notion of "critical" processes ensures that GRC activities will be focused where there is the most leverage. The next step is to identify process owners who should be trained and certified on business process management techniques. The third step is to build and maintain the following information for critical processes:

- Process documentation (e.g. process flows and process maps)
- Process objectives and measurement
- Control plans
- Risk and control assessment
- Change control
- Corrective action

Your technology solution can be a great help in collecting and documenting this information. Process hierarchies should be modeled directly in the GRC repository and related information such as process diagrams, objectives and performance metrics should be stored directly with the process hierarchies.

Since risk events frequently result from handoffs between organizations, an end to end view of key processes is required to better understand and manage cross-organization risks. In addition, firms should focus on end to end process performance. Local mitigation decisions may optimize on the wrong things, for example reducing delays on a process step that is not on the critical path.

Firms should also focus on standardization of key processes across organizations. This can streamline GRC activities since risk and control frameworks will not have to be re-invented for key processes in every organization. This will simplify risk assessments and the aggregation of risk measurement data across the firm.

## The Role of Technology

Meeting the increasing demands of GRC in a large organization requires effective technology support to manage enterprise risk in a rigorous and systematic way — across the entire business. The right technology solution can help your organization:

- Create a central platform to pull all of the different data elements together and maintain the relationships between elements (RCSA, Loss Events, KRIs, Issue Management, Policy Management, etc.)
- Establish a common taxonomy and library for policies, processes, risks, controls, regulatory requirements and other key data elements
- Integrate multiple areas of risk (operational, compliance, strategic, etc.) to provide aggregated analysis and full reporting of all risks across the enterprise
- Provide real-time decision support such as the ability to highlight and provide notifications of trends, exceptions, unusual activities, etc.
- Drive accountability, assign responsibilities and ensure risk management practices are carried out consistently across functional groups and product lines
- Provide a means to effectively manage and automate communication and escalation of risks and issues throughout the organization
- Localize views for different functions/roles and synchronize the activities of the different functions

Be leery of technology solutions that have loosely integrated components for addressing the key risk management activities. It will be difficult to achieve the efficiency benefits of risk convergence if you cannot easily share data across activities and have reporting and workflows span activities.

## Conclusion

GRC convergence presents an opportunity to maximize the cost benefit of risk management processes while at the same time increasing the effectiveness of risk management through a holistic view of risk across disciplines. Achieving these goals requires an ability to easily embed risk management into a firm's everyday business processes and the enabling technology platform must have a high degree of configurability to adapt to a company's unique risk management methodology.

Thus, meeting the increasing demands of GRC in a large organization requires effective technology support to manage enterprise risk in a rigorous and systematic way — across the entire business. Technology can play a critical role in an organization's success in developing and implementing an integrated GRC framework, but it should be used as an enabler, rather than to prescribe process and methodology.

## References

Richardson, Chris, Ernst & Young, "Risk Convergence, Survey Summary and Sample Case Studies." OpRisk USA 2008.

COSO II ERM Framework. www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

Olson, Mark, Federal Reserve Governor (Reuters, April 2006)

OpenPages

201 Jones Road, Waltham, MA 02451
Tel: 781.647.3800 Fax: 781.647.4300
Web: www.openpages.com

WP2120508