Improve your business performance

Transform your governance, risk and compliance program
Contents

Evolving expectations for governance, risk and compliance (GRC) programs ............................................. 1

Key transformational levers to realize savings and improve business performance:
  Using an integrated risk management approach .......... 2
  Simplifying GRC processes ..................................... 4
  Embracing GRC technology .................................... 8

Improve business performance through GRC transformation ................................................................. 11
Evolving expectations for governance, risk and compliance (GRC) programs

As growth expectations intensify, regulation increases and more technology innovations enter the market, GRC programs must continually reassess how to effectively and efficiently meet key strategic objectives. Amid these challenges, most organizations’ GRC functions are still struggling to provide the expected value, both in fulfilling its tasks and realizing savings.

Based on our experiences serving our diverse client base, we have found that these levers were critical in enabling successful GRC transformations that improve business performance:

 Organizations today are struggling with managing risks across the enterprise. Rapidly changing business trends and technological innovations have significantly changed the risk landscape. Companies lagging behind the innovation curve, increase their vulnerability to these proliferating risks.

Using an integrated risk management approach
The ability to anticipate, respond and continually adapt to risk continues to be critical for an effective GRC program – yet various functions (such as internal audit, internal controls and compliance) are not aligned with strategic risks and business performance measures. Executives of leading organizations are placing a greater importance on identifying, managing and monitoring the rapidly evolving strategic and business risk profile, focusing beyond financial, operational and regulatory compliance. Understanding the drivers and impact of risks makes it easier to optimize compliance activities, investment strategies and capital allocations as well as identify and drive process improvement opportunities.

Simplifying GRC processes
To enhance decision making and avoid unnecessary costs, establishing a comprehensive enterprise-wide risk and control governance model is crucial, ensuring that the corporate risk strategy is balanced and that responsibilities for risk oversight and ownership are rightsized and properly defined. Companies with successful GRC programs continue the convergence of their GRC functions by aligning their mandates and scope, coordinating infrastructure and people, and leveraging consistent methods and practices.

Embracing GRC technology
Leading organizations recognize that technology is essential to execute processes effectively and efficiently. GRC technology offers inherent functionality that can help drive optimization and standardization through automation and centralization, which further ensures success of a GRC program.
Using an integrated risk management approach

Traditionally, an organization’s primary GRC focus has been on tactical financial and regulatory compliance activities, which were the responsibility of internal audit, internal controls, compliance, enterprise risk management (ERM) and other functions.

Before an organization can align those functions and enable a more successful GRC program, it must clearly understand risk types. The Robert Kaplan and Anette Mikes risk framework1 lays out three distinct categories of risk and potential responses:

1. **Preventable risks** are financial and operational risks that an organization is focused on eliminating, avoiding, mitigating or transferring in a cost-effective manner, because the only outcomes when an event occurs are monetary fines and negative impact to the company’s reputation. Examples include inaccuracy of financial statements and regulatory noncompliance resulting in fines. Risk aversion is the only way to address these risks. Organizations have made significant investments in designing the controls to mitigate these risks, which are the primary responsibility of various functions, such as internal audit, internal controls, legal compliance and others.

2. **Strategic risks** stem from management’s business gambles. There is “no reward without risk”. Running a business is about taking risk; however, management would like to benefit from the upward potential of risk while avoiding the negative impact of these risks at the same time. Eliminating these risks, or transferring them, is therefore not an option. It is a balancing act which requires the organization to have risk management (as opposite to controls management) in place. These risks include growth through acquisitions and expansion into emerging markets; and managing the risks requires the selection of the right strategic risks to take, establishing risk tolerances, predicting what is going to happen, and monitoring key risk indicators.

3. **External risks** are those outside of organization’s control. The main response to these risks is to limit exposure if a risk event occurs. Examples include natural disasters or economic factors like a recession. Potential risk responses include scenario analysis and stress testing to verify that the organization has the minimum resources to weather the full impact of an external risk event.

---

Once an organization understands its risk types, it can adequately manage them by designing risks responses and control models, shown above. With those in place, a company should consistently align all functions to its strategic risks and business performance measures – creating an integrated approach that can optimize investment strategies and capital allocations as well as identify and drive process improvement opportunities. Executive management should own the process of identifying, managing and monitoring overall risk to the organization, while all the lines of defense must execute the organization's response, with a clear responsibility matrix for the various governing bodies.

### Types of risks and their control models

<table>
<thead>
<tr>
<th></th>
<th>Preventable risks</th>
<th>Strategic risks</th>
<th>External risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Risks arising from within the company that generate no strategic benefits. These risks only cost money when an event occurs.</td>
<td>Risk arising from within the company and are taken for superior strategic returns. No reward without risk taking.</td>
<td>Risk originating outside the company. These risks are uncontrollable.</td>
</tr>
<tr>
<td><strong>Objective</strong></td>
<td>Eliminate, avoid, mitigate or transfer the risks in a cost-effective manner</td>
<td>Use cost-effective risk management to balance the mitigation of risks (protect against downward potential) and value creation (risk taking to benefit from the upward potential)</td>
<td>Reduce the negative impact of an risk event and bring the business back to “business as usual” as soon as possible</td>
</tr>
</tbody>
</table>
| **Control model** | Develop mission statement, rules and boundary systems and diagnostic control systems for standard operating procedures, internal controls and internal audit | Hold interactive discussions about risks to strategic objectives, drawing on tools such as:  
  - Maps of likelihood and impact of identified risks  
  - Key risk indicator (KRI) scorecards  
  - Belief systems and interactive control systems | “Envision” risks through:  
  - Tail-risk assessments and stress testing  
  - Scenario planning  
  - War gaming |

[1] Preventable risks  
[2] Strategic risks  
[3] External risks
Organizations continue to invest in new techniques such as advanced analytics and GRC technologies to help improve processes associated with managing tactical financial, operational and compliance risks. However, for strategic risk management, most organizations continue to operate under traditional enterprise risk management models, which are often not aligned to the current business strategy and risk tolerance of the organization. Aligning the multiple functions responsible for risk in how they handle strategic and preventable risks and standardizing key elements of their processes will make decision-making quicker and more effective, as well as help avoid unnecessary costs.

The following core risk strategy components are critical:

1. **Enterprise-wide risk and control governance model**
2. **Risk building blocks focused on risk strategy, identification, assessment and governance**
3. **Convergence of GRC functions and activities**

### 1. Enterprise-wide risk and control governance model

A crucial step is establishing a comprehensive enterprise-wide risk and control governance model, which requires an effective executive sponsor and clear ownership and accountability for the GRC program. An effective risk governance model ensures that the corporate risk strategy is balanced and that responsibilities for risk oversight and ownership are rightsized and properly defined. This also improves the monitoring required to support the various levels that make up the governance structure. A formal governance model sets the risk culture tone at the top and permeates through all levels of the organization.

**An illustrative example of a comprehensive risk governance structure**

<table>
<thead>
<tr>
<th>Board of directors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk committee</td>
</tr>
<tr>
<td>Other committees</td>
</tr>
<tr>
<td><strong>CEO</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk management executive committee</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFO</td>
</tr>
<tr>
<td>CAO</td>
</tr>
<tr>
<td>CRO</td>
</tr>
<tr>
<td>CIO</td>
</tr>
<tr>
<td>CAE (observer)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business unit presidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>BU 1</td>
</tr>
<tr>
<td>BU 2</td>
</tr>
<tr>
<td>BU 3</td>
</tr>
</tbody>
</table>

**Why?**

- Establish accountability and remove ambiguity — everyone has a role in risk management
- Measure performance and rewards on a risk-adjusted basis — what gets measured gets done
- Enable risk communication through formalized channels
- Move from a single-value, hindsight-based evaluation of performance to a forward view of the range of uncertainty and what the business is doing to reduce uncertainty
2. Risk building blocks focused on risk strategy, identification, assessment and governance

To be effective, the enterprise-wide risk and control governance model must be enabled by following building blocks:

► **Formal risk strategy addressing vision and appetite**
  A comprehensive risk strategy enables informed decision making and creates alignment and consistency in the undertaking of risks. It also helps eliminate excessive risk aversion and related opportunity costs. This risk appetite is visible, tangible and can be shared with stakeholders, which enhances vital decisions made during the course of business.

► **Formal risk identification process**
  Most companies face challenges in how to quickly and effectively respond to new or changing risks. The risk management process is always in a continuum and requires constantly monitoring. To minimize uncertainties, organizations need the infrastructure to implement a response with a formal process that allows management to:
  ▶ Effectively identify the type of risk and assess the impact on the organization
  ▶ Define the required risk response (for example, avoidance, elimination, limiting exposure or monitoring/managing to maximize returns based on type of risk)
  ▶ Communicate the organization’s risk posture comprehensively to all the stakeholders

► **Risk assessments**
  Organizations should leverage assessments to establish an aggregated view of risks aligned to strategy and risks to performance. A structured analysis of risks to value can comprehensively identify exposures that threaten an organization’s ability to achieve its strategic and operational goals.

► **Risk governance**
  Risk governance practices ensure that the corporate risk strategy is properly balanced across the organization and that responsibilities for risk oversight and ownership are clearly defined, aligned and monitored. A strong risk management process is only as effective as the executive sponsorship and the embedded risk culture of the company.
3. Convergence of GRC functions and activities

Comprehensively aggregating identified strategic, preventable and external risks, as well as consolidating risk governance and compliance activities, will further improve GRC processes. This will also help achieve long-term cost savings by eliminating duplication; enhancing efficiency in strategic, financial and operational risk management activities; and boosting the organization’s ability to keep pace with essential business growth and transformational initiatives.

Companies that converge their GRC functions can effectively challenge the efficiency and effectiveness of their compliance activities across the organization. Consolidating and standardizing activities under internal audit, internal controls, legal compliance, ERM and others decreases costs, drives enhanced integration, and maximizes the value of risk management activities.

This enterprise-wide initiative should compile the driving imperatives from the board and executive management as well as other relevant functions. These imperatives should also include the strategic business and operational processes as well as the external and internal

The following statement made by the controller of a Fortune 100 company is the resounding theme for many companies:

“We have exhaustive disparate controls and compliance activities taking place in the company led by different people adopting different process and technology solutions, and my main concern is that I do not have visibility in how these activities interrelate or complement each other, nor do I know where the gaps may exist.”

Current state

<table>
<thead>
<tr>
<th>Board oversight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit committee</td>
</tr>
<tr>
<td>Risk committee</td>
</tr>
<tr>
<td>Other committees</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internal audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management</td>
</tr>
<tr>
<td>Compliance</td>
</tr>
<tr>
<td>Internal control</td>
</tr>
<tr>
<td>Information technology</td>
</tr>
<tr>
<td>Legal and regulatory</td>
</tr>
<tr>
<td>External audit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business unit</td>
</tr>
<tr>
<td>Business unit</td>
</tr>
<tr>
<td>Business unit</td>
</tr>
</tbody>
</table>
assurance requirements. Standardizing these requirements enables the organization to build a more integrated GRC ecosystem with standardized GRC data and fosters a common language (e.g., risk catalog, process hierarchy and definitions).

When the below-mentioned core risk strategy components are in place, companies can realize the following benefits of an enhanced and optimum risk strategy:

- **Risk and compliance convergence leading to cost savings**
  Convergence and alignment of risk functions significantly reduce compliance spend and reduce the burden of monitoring at the department and process level, leading to increased and better risk coverage.

- **Decision making supported by advanced risk analytics and monitoring**
  Alignment of risks with performance metrics and risk targets supports continuous monitoring of risk exposures and targeted improvements to business processes. Comprehensive data mining and analytics are required to effectively monitor and report on these strategic business risks to allow executive management to effectively manage the impact on rate of return and financial performance of the organization.
Embracing GRC technology

GRC technology solutions are a critical enabler of effectively and efficiently executing GRC processes and providing one risk management language, consistency and integration. However, most organizations continue to underutilize them. Traditionally companies adopted GRC tools as a quick resolution to an immediate issue; for example, implementing a “segregation of duties” monitoring solution to resolve an audit finding. As a result, broader applications of GRC tools and return on investment analysis were not always considered, therefore limiting their applications and value.

Leading organizations have recognized this opportunity as a strategic imperative and enable their GRC transformation with technology solutions. As a result, they improved their process execution by:

- Automating and standardizing processes and controls
- Embedding and maintaining one single version of risk and control data
- Managing holistic views of risk and compliance exposures
- Generating dynamic and real-time risk and control intelligence and reporting
- Analyzing risk-driven indicators and exception-based decision making
- Escalating through different levels of the organization via work flow

Key transformational levers to realize savings and improve business performance

Client issues and risk framework

Enhance risk governance

- Risk strategy and alignment
  - Improve the overall alignment of risk with corporate goals, major initiatives and emerging market trends
  - Clarify the definition of “risk,” and determine management and the board’s risk appetite and overall tolerance levels
  - Communicate overall risk strategy to key stakeholders

- Risk oversight and accountability
  - Clarify and strengthen risk oversight at the board and executive management levels
  - Deliver greater transparency and accountability at all levels in the organization

Embed risk management

- Risk prioritization
  - Define the key “risks to own” that drive growth and create value (day-to-day business, change programs, emerging business)
  - Invest differentially in the strategic “risks that matter” to better enable performance

- Risk linkage to the business
  - Link risk management to business planning and performance management
  - Align key risk indicators (KRIs) with KPIs and key control indicators (KCIs)

Enable risk management

GRC technology enhances risk management, controls and processes execution by:

- Consolidating risk management activities across the organization
- Enabling continuous process and controls monitoring
- Providing reports and dashboard to enhance visibility to leadership, facilitating rapid response to risk events

Improve controls and processes

- Controls and process optimization
  - Reduce cost of controls spend
  - Increase the use of automated controls vs. manual controls
  - Implement more prevent controls vs. detect controls
  - Optimize controls around key business and IT processes

- Compliance
  - Monitor critical controls and KPIs continuously to ensure regulatory compliance

Optimize risk management functions

- Individual risk management functions
  - Improve the effectiveness and efficiency of individual risk management functions

- Alignment/coordination of risk functions
  - Reduce redundancies and overlap in risk coverage
  - Coordinate risk activities and align skills to better leverage existing infrastructure and resources
Companies that have successfully leveraged GRC technology have attributed their achievements to:

- **Executive sponsorship that spans business and IT**
  Executive sponsorship helps to clearly align the business requirements of the overall GRC program to the appropriate GRC technology or technologies. It is a critical step in establishing a common platform for multiple GRC functions and mandates.

- **Comprehensive business case**
  Developing a thorough, convincing business case clearly establishing return on investment is critical to achieving the full value of any GRC program, especially those enabled by a GRC technology solution, which typically requires substantial investment. The business case must clearly identify financial, operational and qualitative benefits to the organization, which will help validate organizational alignment challenges and adequately prioritize it against other company initiatives.

- **Multi-year GRC road map merging GRC program activities with GRC technology enablement**
  A comprehensive GRC program enablement is typically a complex, multi-year project, requiring alignment from a broad spectrum of stakeholders. A clear road map, integrating all elements of the program, including technology, can help visualize the journey and define key milestones and integration points.

---

**Key GRC decisions**

- Scope
- Risk management strategy
- Organizational ownership decision
- Procedures and standards
- Project management
- Monitoring strategy
- Testing strategy
- Reporting and analytics
- Training

Executive leadership teams define the GRC implementation strategy and are responsible for providing direction and driving consistency and accountability during system and process design.

The operational teams are responsible for ensuring that the strategic vision defined by leadership is embodied in the implementation plan. The team identifies the specific improvement opportunities and develops the methodology to implement the change.

The execution teams (this could comprise of the enterprise security team, the GRC technical team and key stakeholders of the end-user base) are tasked with developing processes and technology definitions that are effective and sustainable, to adhere to the long-term strategic and operational objectives of the GRC strategy.

**An illustrative example of how to align a GRC implementation to overall GRC program objectives.**
Opportunities exist to transform your governance, risk and compliance program to realize savings and improve performance.

Leading companies have achieved successful results by focusing on:
- Shifting risk management focus to a cross-functional approach aligned to strategic risks and business performance measures
- Standardizing GRC processes to enhance decision making and avoid unnecessary costs
- Embracing GRC technology to execute processes effectively and efficiently

It's time to act now and position your company for long-term success.

<table>
<thead>
<tr>
<th>Call for action</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you have a comprehensive risk vision and strategy?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have your risk vision and strategy addressed the three main risks: external, strategic and preventable?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your board have confidence that you understand their risk vision and appetite?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have you established your risk appetite and tolerance for strategic risk events that could provide upward or downward potential to the business?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have visibility into the risk coverage of the company?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you confident that there are no gaps in risk coverage and that they have visibility into how issues roll up and impact the strategic business risks?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you confident that risk responses and compliance activities are optimized across the organization?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you effectively leverage GRC technology to support your GRC program?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If the answer to any of these questions is “no,” it is time to take action.
Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our Insights on governance, risk and compliance series at www.ey.com/GRCinsights

Want to learn more?

Expecting more from risk management: drive business results through harnessing uncertainty. www.ey.com/repm

Getting value out of your lines of defense: a pragmatic approach to establishing and optimizing your LOD model. www.ey.com/lod

Unlocking the power of SAP’s governance, risk and compliance technology. www.ey.com/sapGRC

Centralized operations: the future of operating models for Risk, Control and Compliance functions. www.ey.com/centralops


Step up to the challenge: helping Internal Audit keep pace with a volatile risk landscape. www.ey.com/IArisks
At EY, we have an integrated perspective on all aspects of organizational risk. We are the market leaders in internal audit and financial risk and controls, and we continue to expand our capabilities in other areas of risk, including governance, risk and compliance as well as enterprise risk management.

We innovate in areas such as risk consulting, risk analytics and risk technologies to stay ahead of our competition. We draw on in-depth industry leading technical and IT-related risk management knowledge to deliver IT controls services focused on the design, implementation and rationalization of controls that potentially reduce the risks in our clients’ applications, infrastructure and data. Information security is a key area of focus where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing.
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2014 EYGM Limited. All Rights Reserved.

EYG no. AU2558
ED none

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/GRCinsights

About EY’s Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business, having the right advisors on your side can make all the difference.

Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view: ey.com/advisory

The leaders of our Risk practice are:

### Global Risk Leader

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paul van Kessel</td>
<td>+31 88 40 71271</td>
<td><a href="mailto:paul.van.kessel@nl.ey.com">paul.van.kessel@nl.ey.com</a></td>
</tr>
</tbody>
</table>

### Global Risk Transformation Leader

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matthew Polak</td>
<td>+1 412 644 0407</td>
<td><a href="mailto:matthew.polak@ey.com">matthew.polak@ey.com</a></td>
</tr>
</tbody>
</table>

### Area Risk Leaders

**Americas**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amy Brachio</td>
<td>+1 612 371 8537</td>
<td><a href="mailto:amy.brachio@ey.com">amy.brachio@ey.com</a></td>
</tr>
</tbody>
</table>

**EMEIA**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jonathan Blackmore</td>
<td>+971 4 312 9921</td>
<td><a href="mailto:jonathan.blackmore@ae.ey.com">jonathan.blackmore@ae.ey.com</a></td>
</tr>
</tbody>
</table>

**Asia-Pacific**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iain Burnet</td>
<td>+61 8 9429 2486</td>
<td><a href="mailto:iain.burnet@au.ey.com">iain.burnet@au.ey.com</a></td>
</tr>
</tbody>
</table>

**Japan**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yoshihiro Azuma</td>
<td>+81 3 3503 1100</td>
<td><a href="mailto:azuma-yshhr@shinnihon.or.jp">azuma-yshhr@shinnihon.or.jp</a></td>
</tr>
</tbody>
</table>