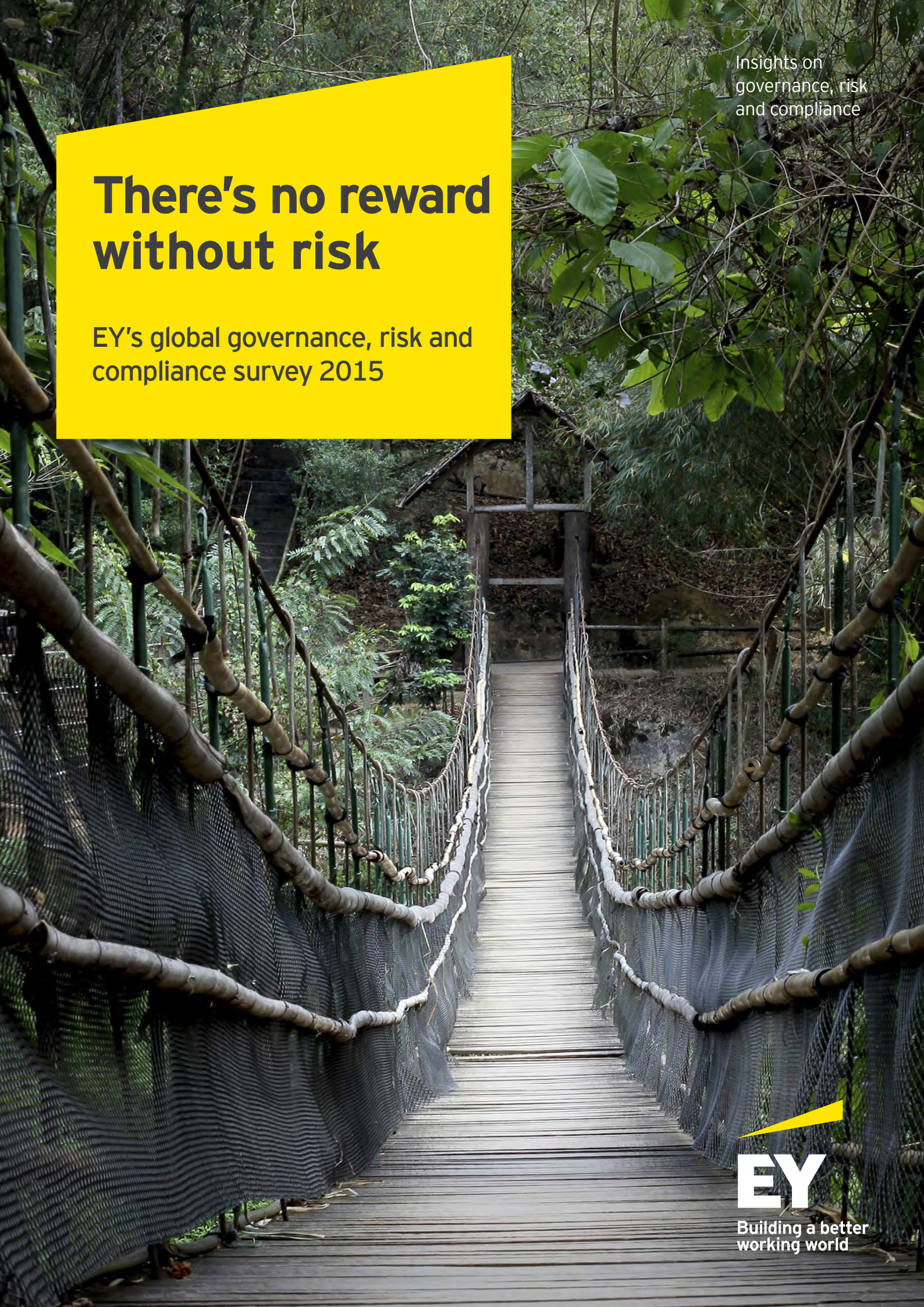


Insights on governance, risk and compliance

There's no reward without risk

EY's global governance, risk and compliance survey 2015

Building a better working world

Contents

Welcome

Welcome to ***There's no reward without risk***: our thought leadership report based on the findings from our global governance, risk and compliance survey 2015.

Operating a business requires taking risks. Organizations that identify and manage these risks well are positioned to grow and remain successful. In this year's survey, we asked 1,196 participants, around the globe and across sectors, how well they are managing risk and what they need to do to better manage the risks that drive performance.

Organizations today are challenged with managing a rapidly changing risk landscape. Reports in the media illustrate the increasing risks faced by organizations: market volatility, geopolitical crises, wide-spread economic changes, regulatory reforms and cyber threats. Long-term patterns such as the aging population, the rise of hyper connectivity and increasing geographic mobility are also having a direct effect on organizations worldwide.[1] While this creates many challenges for organizations, it also presents an opportunity to take advantage of the upside potential of risk.

In this year's survey, we found that organizations are making progress in improving the way they manage risk in response to a changing risk landscape. However, organizations also indicated that there is still further room for improvement and opportunities to be seized. However, this requires businesses to change the way they work and how they capitalize on it, so that they become a more risk-aware organization. This report captures EY's perspectives on how businesses should do that.

We hope that you enjoy reading our insights and we would like to extend a personal note of thanks to all of our survey participants. We appreciate the time they took to share their experiences.

Every organization takes risks; let's discuss how to best manage them together.

"Every challenge and every opportunity an organization faces today demands change. And with change comes risk. We help our clients see all sides of risk: find where there's opportunity in risk, protect against the risk you can see and identify risks you don't know about yet."

Paul van Kessel, Global Risk Leader

Paul van Kessel
EY Global Risk Leader
paul.van.kessel@nl.ey.com

Matt Polak
EY Global Risk Transformation Leader
matthew.polak@ey.com

Michael O'Leary
EY Global Internal Audit Leader
michael.oleary@ey.com

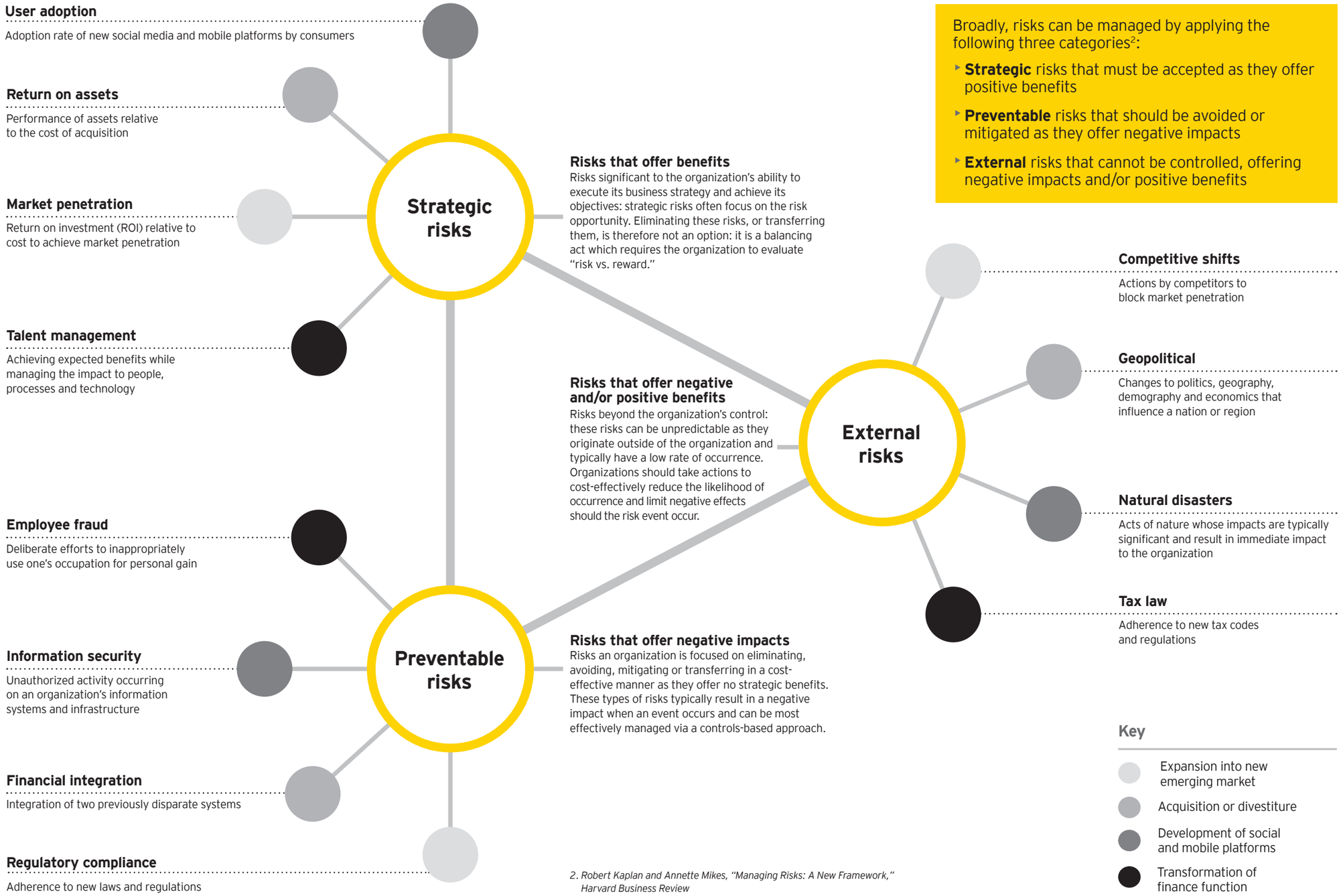
1. Global Risks Perception Survey 2014, World Economic Forum

Looking at risk differently

Historically, risks have been categorized in many different ways. We believe that regardless of how they are organized, it is beneficial to consider risks in the context of your business and how best to respond to those risks.

By categorizing risks according to their impact to the business, organizations are able to shift their focus with regard to how they identify and respond to the risks they face – both internal and external, as well as those with positive and negative impacts – and best respond to each risk appropriately.

Until now, organizations have primarily focused on risks that can be managed through the implementation of controls, but offer little to no upside or benefit. However, with increasing stakeholder demands and an ever-evolving business landscape, leading organizations are now focusing more of their time and efforts on managing the risks that impact value creation.



Broadly, risks can be managed by applying the following three categories[2]:

- **Strategic** risks that must be accepted as they offer positive benefits
- **Preventable** risks that should be avoided or mitigated as they offer negative impacts
- **External** risks that cannot be controlled, offering negative impacts and/or positive benefits

2. Robert Kaplan and Annette Mikes, "Managing Risks: A New Framework," Harvard Business Review

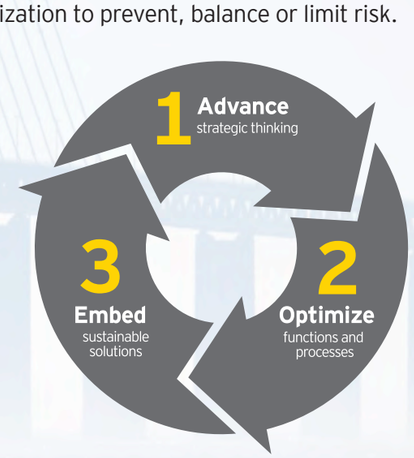
Building a risk-aware organization

Identifying, managing and responding to risk should be an integral part of an organization's everyday activities. This can be achieved by applying the three risk categories: strategic, preventable and external.

Our global governance, risk and compliance (GRC) survey tells us that organizations are looking for a more comprehensive, coordinated and innovative approach to enable them to successfully manage the opportunities and the hardships presented by risk. This requires transforming the way the organization views and capitalizes on risk — we call this "building a risk-aware organization."

With the knowledge that risks are a never-ending challenge and new risks will be encountered every day, a stepped approach to risk management is required:

- **Step 1. Advance strategic thinking**
  The first step challenges the way organizations categorize, manage and respond to risk: thinking about risk in the context of their business decisions and designing risk response plans to appropriately manage identified risks.
- **Step 2. Optimize functions and processes**
  The second step focuses on what organizations are doing to optimally align functions by allocating talent and design risk management processes to efficiently and effectively execute risk response plans across each of the lines of defense (see page 12).
- **Step 3. Embed solutions**
  The third step highlights the importance of integrating sustainable solutions throughout the organization to prevent, balance or limit risk.



Advance

- Identify and assess risks that impact business strategy
- Design risk response to reduce the downside and take advantage of the upside potential

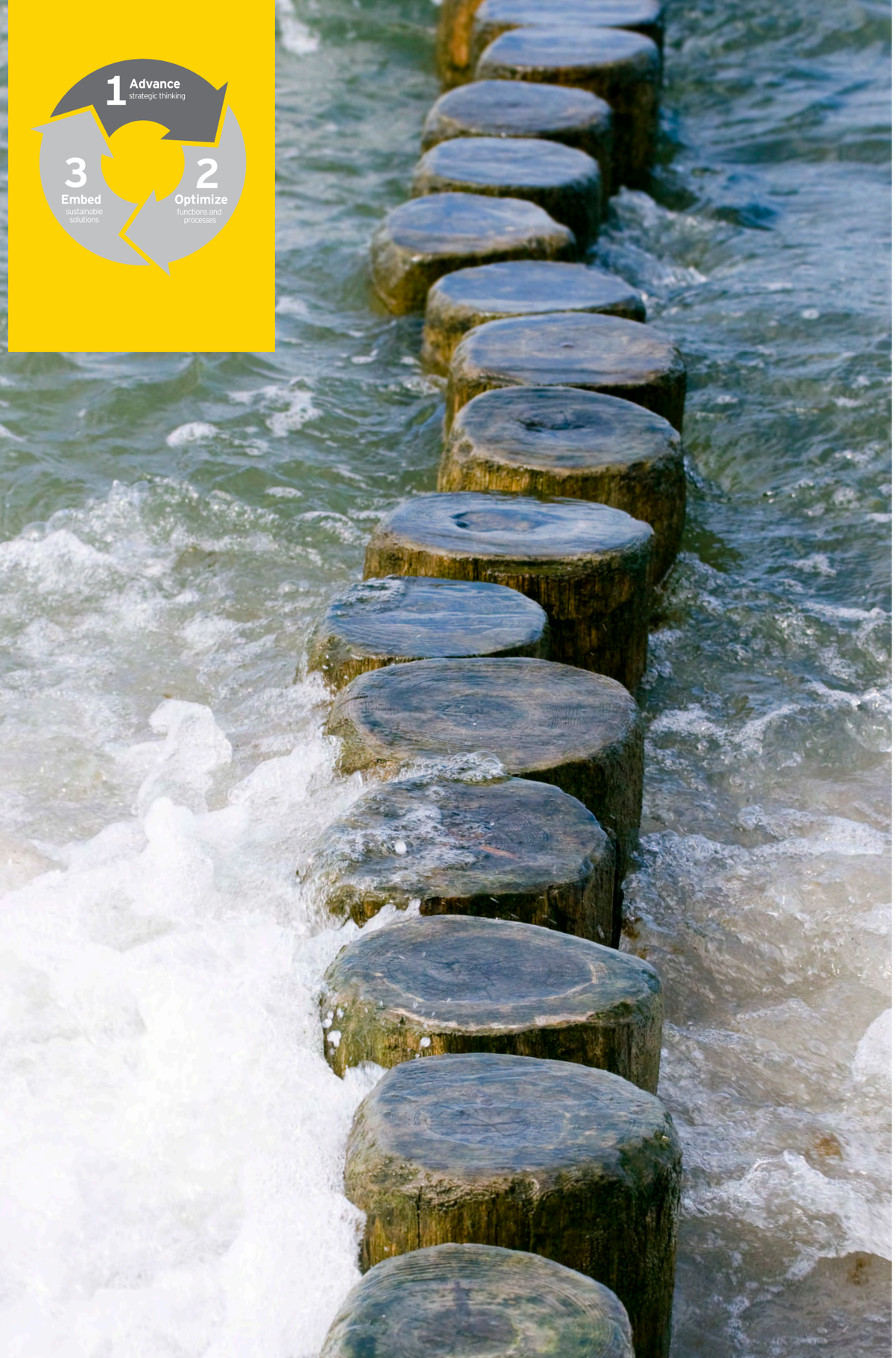
Optimize

- Optimally align functions to execute the organization's risk response plans/strategy
- Develop risk processes to facilitate better coordination, communication and reporting

Embed

- Design solutions that prevent, balance or limit risk
- Implement technologies to effectively execute and sustain the solutions

These three steps are explained further in the following pages.



Advance strategic thinking to improve value creation

Organizations are not created to manage risk, they are created to generate value as part of a broader aspirational purpose; as a result, they need to focus on the risks that directly impact their purpose and business strategy.

Organizations that methodically identify, assess and respond to the risks that impact their business strategy are better equipped to define risk responses that reduce the negative impact of risk while maximizing its upward potential. They think strategically about risk.

Organizations that exhibit advanced strategic thinking:

1. **Identify and assess the risks that impact their business**
2. **Design risk response plans**

77%

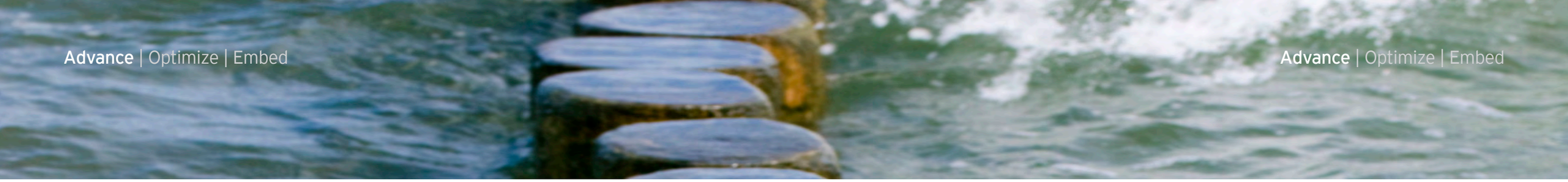
of respondents evaluate their organization's risk profile on an annual basis, limiting their ability to adjust their business strategy based on changes to their risk landscape.

1. Identifying and assessing the risks that impact your business

Organizations need to continuously evaluate their business strategies and determine the level of risk exposure they are willing to accept to generate value, otherwise known as their risk appetite. This approach better enables organizations to effectively and methodically identify and assess their risk landscape in the context of their business, as depicted in the graphic on page 2. In this year's GRC survey, 77% of respondents only evaluate their organization's risk profile on an annual basis, limiting their ability to adjust their business strategy based on changes to their risk landscape.

In the table below, some of the potential risks associated with each business strategy are identified, applying the three risk categories – strategic, preventable and external. Each business strategy requires taking a strategic risk in search of higher reward (e.g., high ROI). They each also introduce preventable risks that must be dealt with as a result. Lastly, external risks may exist that could negatively impact each strategy.

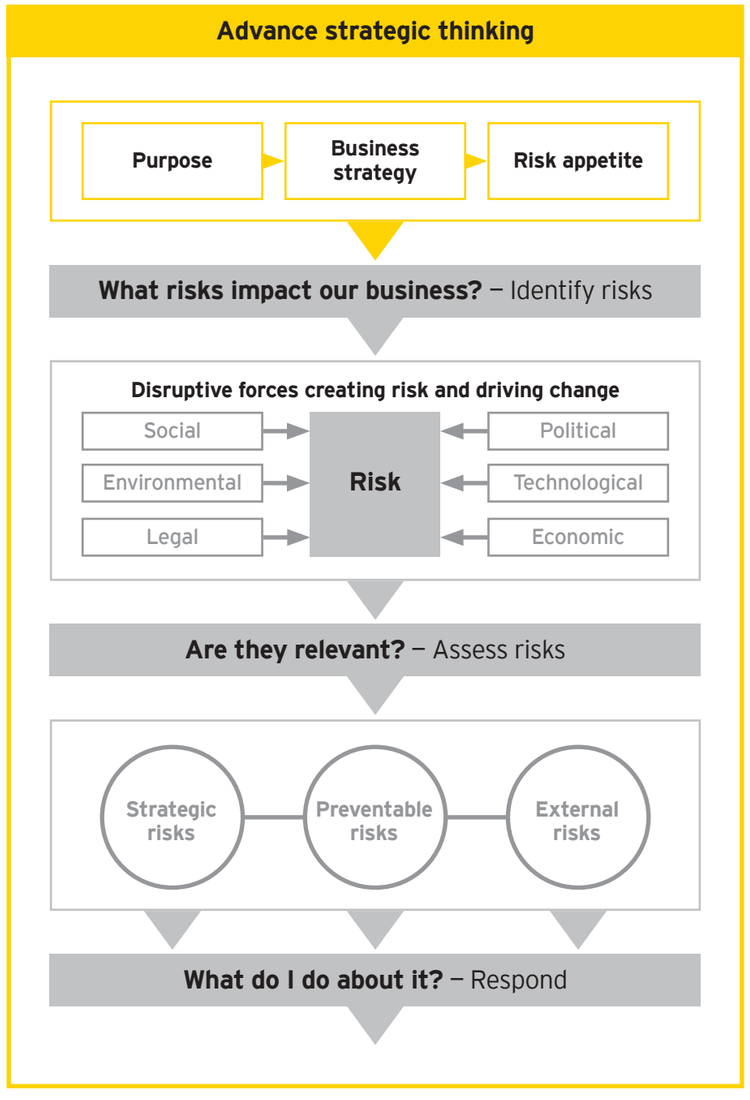
Business strategies	Strategic risks	Preventable risks	External risks
Expansion into new and emerging markets	Minimal ROI in new sales and distribution channels	Non-compliance with new legal and regulatory requirements	Government actions to block market penetration or expansion
Acquisitions or joint ventures	Underperforming assets acquired through acquisition	Failure to detect accounting or financial irregularities	Political reform or action blocking M&A transactions
Development of social and mobile platforms	Low adoption rate of digital platforms by consumers	Disruption to customer interfaces and transactions	Natural disaster impacting IT supporting infrastructure
Transformation of finance and accounting functions	Disruption to business and customer support processes	Changes to existing risk and controls framework	Economic shift requiring cuts to capital expenditure



Advance | Optimize | Embed

"Companies that think about risk in the context of their business decisions are better positioned to manage the risks that drive performance."

Matt Polak, EY Global Risk Transformation Leader



An organization needs to assess each identified risk to determine its likelihood, potential impact or time to realization. For example, the likelihood of a natural disaster (an external risk) occurring that could negatively impact critical IT infrastructure may be low, but the potential impact to an organization launching new customer-facing IT platforms could be catastrophic.

In another example, the likelihood and impact of disruptions to business and customer support processes arising as part of a major transformation program (a strategic risk) may be relatively high; but the benefits associated with such a program are also significant.

To make the right assessments, organizations need to directly address risk management in strategic and business planning discussions. They also need to routinely evaluate their risk profile and its impact on their business strategy, enabling the organization to readily identify new and emerging risks and adapt their strategy accordingly.

Getting organizations to think differently about the risks to their business by strategically applying the three risk categories (as depicted in the table and graphic) enables them to identify risks they may not have otherwise thought of. Organizations are able to clearly identify the key risks to "own" that not only result in negative consequences, but also those that generate value, enabling a direct linkage between risk and business performance. It is encouraging that 85% of survey respondents indicated opportunity exists to further improve the linkage between risk and business performance.

2. Designing risk response plans

Once an organization has identified and assessed its key risks, it can manage them by designing cost-effective and efficient risk response plans based on the organization's risk appetite and each risk category – strategic, preventable and external.

For instance, the amount of risk an organization is willing to accept as part of a transformation program may be low, but disruptions to business and customer support processes could negatively impact the organization's reputation/brand and ROI: as a result, the organization must employ cost-effective risk management to balance the mitigation of risk with the expected benefits of the program.

Likewise, an organization may be willing to accept a greater amount of risk in complying with new legal or regulatory requirements if the cost of noncompliance is relatively low or can be avoided all together. An organization developing digital platforms to better interact with its customers can take advantage of the upward potential of risk by not only designing responses to monitor for negative publicity that could harm its reputation, but also design responses that monitor for positive publicity that it can capture and highlight in the marketplace.

Advanced strategic thinking enables organizations to manage the risks that directly impact their business strategy and performance. This strategic approach makes it easier to then coordinate functions, align talent and design processes to support the organization's overall risk strategy.

85%

of respondents indicated opportunity exists to further improve the linkage between risk and business performance.

90%

of respondents indicated their company's risk profile slightly or significantly influences their capital allocations.

Optimize functions and process to effectively execute your risk strategy

Once an organization has determined its risk response plans or strategy, it needs to optimally align its functions, allocate resources and design risk management processes to efficiently and effectively execute its strategy.

Organizations have historically dispersed responsibility for risk activities to specific functions within the organization. This has resulted in silos, negatively impacting the effectiveness of risk management activities by preventing critical information from reaching key decision-makers. If a clear operating model and processes are not defined, then communication does not flow effectively through the organization.

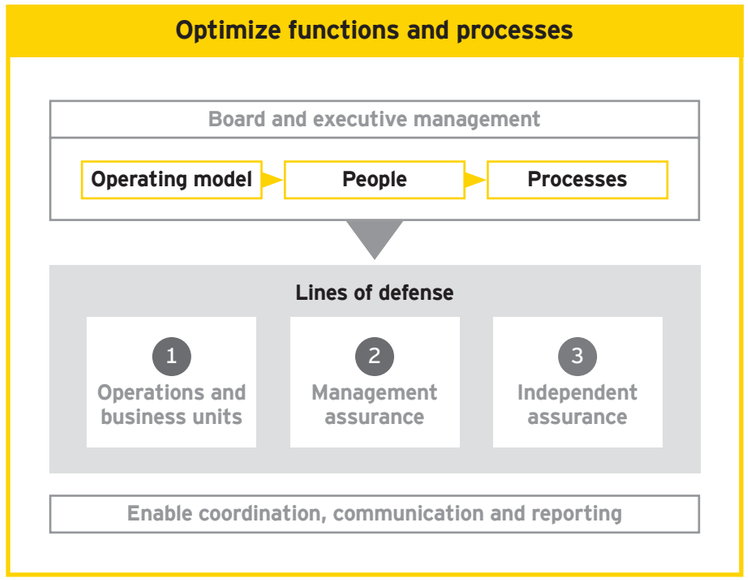
Leading organizations optimize functions and processes by:

1. **Establishing a well-defined and coordinated operating model**
2. **Aligning the right talent and skillsets**
3. **Designing risk management policies and processes**

1. Establishing a well-defined and coordinated operating model

In this year's GRC survey, respondents clearly recognized the value of a well-coordinated operating model; 67% expected activities to be well-coordinated within three years.

Organizations must define clear ownership and accountability for risk activities to enable effective coordination, communication and reporting. Management owns the process of identifying, managing and monitoring overall risk to the organization. Management sets the tone at the top, fosters a risk aware culture and defines the organization's risk strategy.



Respondents identified the following as the top opportunities to enhance the way their organization manages risk:

1. Better alignment of risk objectives with business objectives
2. Clearer risk ownership processes and operating model
3. Improved ability to provide a comprehensive view of risk
4. More structured and frequent risk communications to key stakeholders and decision-makers within the organization
5. More effectively leveraging technology across the organization to efficiently manage risk

"Having the right structure and mechanisms in place, and adapting them as needed, is critical to improve the efficiency and effectiveness of risk activities across the organization."

Michael O'Leary,
EY Global Internal Audit Leader

Advance | **Optimize** | Embed

67%

of respondents expect risk activities to be well-coordinated within three years.

56%

of respondents' organizations have created a chief risk officer position to provide oversight over risk management activities.

Survey respondents overwhelmingly recognized the need for the three lines of defense to work together to manage risk.

The "three lines of defense" need to be identified and deployed as part of the organization's risk strategy. However, no line of defense executes this strategy single-handedly, they must work in concert. EY defines three lines of defense as follows:

- **First line (operations and business units)**
  This group comprises of the line management responsible for identifying and managing risks directly (design and operational controls); they regard risk management as a crucial element of their everyday jobs.
- **Second line (management assurance)**
  This group (typically covering risk management, internal controls, SOX, legal, compliance, etc.) is responsible for the ongoing monitoring of the design and operation of controls in the first line of defense, as well as advising and facilitating risk management activities.
- **Third line (independent assurance)**
  This group is responsible for independent assurance over risk management activities – it will include the Internal Audit function, external auditors and applicable regulators.

The organization's management should be responsible for mapping and assigning clear ownership and accountability for risk response activities across the three lines of defense. This establishes a structure to facilitate coordination, communication and reporting across clear boundaries of responsibility; it also enables an organization to validate risk coverage and foster a culture in which all parties understand their role in executing the organization's risk strategy.

Defining a risk culture

Risk culture is reflected in the behaviors and actions of people. It is the belief system, or set of values within an organization that make risk an integral part of the business and supports the achievement of the organization's overall purpose. Regulators address risk culture through factors affecting risk-taking behavior such as risk appetite, governance and compensation.

To deliver an appropriate risk culture, a variety of mechanisms need to be in place and be effective. When in place and effective, the mechanisms contribute to deliver the desired behavior outcomes.

Attributes of a sound risk culture:

- **Leadership:** Tone from the middle tier of management is aligned with tone from the top tier to establish desired risk behaviors.
- **Organization:** Governance and business models support the delivery of desired risk behaviors and enable strong accountability and effective challenge.
- **Risk framework:** Risk management framework is embedded in the way the business manages risk and enables effective challenge.
- **Incentives:** Employee life cycle and incentives support the delivery of desired risk management behaviors.

2. Aligning the right talent and skillsets

Once an organization has assigned clear ownership and accountability for risk response activities, it needs to then align the resources and skillsets required to execute those activities. This is usually straightforward in the first line of defense, but may be more complex in the second and third line.

Leading organizations demand talent with deep industry and business knowledge, as well as skills relevant to each of the risk categories – strategic, preventable and external. Recognizing the upside potential of strategic risks and the need to limit the potential impact of external risks, these organizations are developing and aligning talent with the requisite skillsets across each of the three lines of defense to improve the effectiveness and efficiency of each, better enabling the organization to execute its risk strategy.

Respondents identified the following as the most important skills or experiences required to enhance their risk functions:

1. Risk management
2. Business strategy
3. Critical/analytical thinking
4. Regulatory compliance
5. Process improvement

As an example, resources with a background in business continuity planning or disaster recovery (DR) have typically resided within the first line of defense, but leading organizations are now embedding resources with similar backgrounds within the first and second lines of defense to facilitate and monitor the response related to external risks. Similarly, launching a new social media platform requires resources with digital expertise within each line of defense; this enables each line to better understand the associated strategic risks and appropriately balance risk mitigation activities with the benefits.

3. Designing risk management policies and processes

Lastly, an organization must design policies and processes governing the execution of its risk response plans. Risk management policies and processes are integral to influencing behaviors, coordinating activities, establishing communication protocols and facilitating risk reporting – they dictate **why to do it**, **what to do** and **when to do it**.

To illustrate, an organization facing external risks arising from competitor strategic shifts might design processes to facilitate wargaming exercises across the three lines of defense to evaluate the potential impact to the company's business strategy. These processes would help to define each function's role and responsibilities, the frequency at which the exercises are conducted, and how the results are to be compiled and communicated to decision-makers.

Optimization of functions and processes helps organizations establish a structure in which it can efficiently and effectively execute its risk strategy. The appropriate operating model, talent, skillsets, and risk management policies and processes enable the smooth execution of risk response activities; making it easier to embed solutions as part of the fabric of the organization.

65%

of respondents do not produce a report, or only prepare an integrated risk management report annually.

3. Embed

Embed solutions to proactively respond to risk and improve performance

Organizations that embed solutions as a core aspect of their business can proactively respond to risk and drive performance.

They execute their risk response plans more effectively and are better enabled to prevent, adapt and anticipate risk that would otherwise impact their business strategy. It is not about adopting one-off solutions, it is about embedding sustainable solutions that enable an organization to remain successful.

Organizations that think strategically about risk and have optimized their functions and processes are able to more easily embed and sustain solutions across the three lines of defense. These solutions are based on the organization's risk response plans and align to the objectives of each risk category – strategic, preventable and external.

Categories of risks: strategic, preventable and external

Risk responses

Preventable risks

Keep it simple: embed solutions that seek to prevent or eliminate these risks all together. Design risk and control frameworks that optimally prevent risks from arising, and can be efficiently monitored and tested to deter or detect risks if they arise.

Organizations implementing new financial platforms should design application security that address compliance requirements and align to the businesses' operating model; eliminating potential risks resulting from segregation of duties conflicts or excessive access at go-live. Leveraging GRC technology, organizations can implement additional control measures to detect and deter potential segregation of duties conflicts from arising. In this case, the second and third lines of defense play a major role in both ensuring that compliance requirements are adequately addressed and assessing the design and operating effectiveness of control measures.

Leading organizations focus on optimizing their internal control frameworks to eliminate duplication and automate controls. Similarly, organizations adopt continuous process monitoring solutions to further enhance and automate controls as well as improve the second and third line's ability to monitor the overall internal control environment. In our GRC survey, 75% of respondents identified usage of continuous monitoring, ranging from fraud detection, transaction monitoring and performance monitoring.

As a result, these types of solutions better enable all parties within the organization to focus their efforts on managing the strategic and external risks.

Strategic risks

Balance risk mitigation with risk taking: embed solutions that reduce potential risks to your business strategy and enable you to adapt should those risks arise.

Organizations willingly accept some degree of risk in order to drive business performance; for example, a financial services organization offering new products needs to accept a defined level of risk associated with extending its products and services to potential high-risk customers. Organizations balance and manage this type of risk through solutions such as risk modeling and analytics. This enables them to monitor the risk exposure to the organization real-time and adjust their business strategy accordingly – in this case, their criteria for accepting customers – capitalizing on the customers they do want to target.

The second and third lines of defense facilitate and monitor the effectiveness of the models and analytics, as well as challenge the inputs and underlying assumptions. As new products are offered, the criterion by which customers are evaluated is continuously updated, reducing the risk to the organization while reaping the expected benefits.

49%

of respondents utilize one or more GRC technologies to enable risk management activities.

Audit and compliance management, security and process controls and enterprise risk management capabilities are viewed as the most important GRC technology capabilities today.

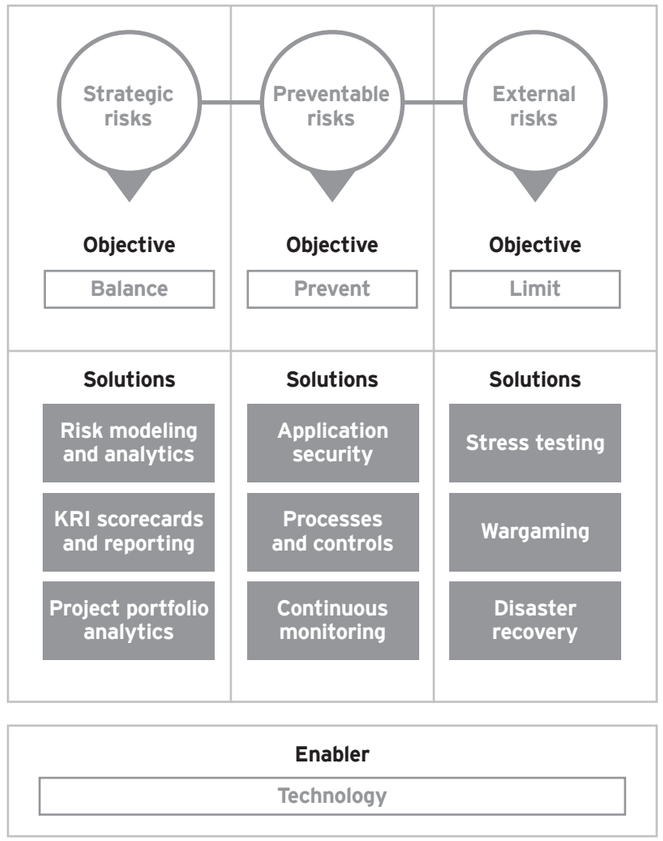
Advance | Optimize | **Embed**

Respondents identified the top activities enabled through continuous monitoring as:

1. Controls monitoring/ testing
2. Fraud detection
3. Security monitoring
4. Transaction analysis
5. Compliance monitoring

Leading organizations prepare scorecards, dashboards and other forms of reporting – including monitoring key risk indicators (KRIs), key performance indicators (KPIs) – for the board and executive management. This provides visibility into the risks that impact their business strategy and how they will affect the organization's overall risk profile, enabling management to adapt the organization's business strategy as appropriate. However, 78% of our GRC survey respondents only prepare management dashboards annually or quarterly, indicating further opportunity exists to provide decision-makers with vital risk insights more regularly.

Embed solutions



Case study

An organization transforming its finance function into a shared services center operating model to improve its bottom line, willingly accepts the risks associated with changing operational processes, organizational structures and systems. The changes are required to realize the expected benefits, but pose potential risks that ultimately impact the overall ROI. Solutions such as project predictive analytics or benefits monitoring can effectively manage and balance the risks associated with such a transformational program. The second line of defense working in collaboration with the first line, assists in evaluating the program's overall management and execution to anticipate and adapt to risks as they arise, balancing risk with ROI. The third line of defense embeds experts within the program to proactively identify and monitor the mitigation of high-risk areas.

External risks

Prepare for the worst, hope for the best: embed solutions that anticipate and limit the impact of external risks. These solutions enable organizations to regularly identify potential risks, assess their impact, determine how to limit it and help to bring the organization back to "business as usual."

Stress testing, scenario planning and wargaming enable organizations to assess the impact of outside forces on their business strategy. For example, an organization periodically conducts scenario planning to analyze the impact of forces such as geopolitical crises, technological shifts, regulatory changes or economic volatility on their business within the next 5 to 10 years. The second line of defense facilitates these exercises along with participants from the first line to assess how the organization would perform under different scenarios. The third line of defense participates within the exercises acting as an advisor, providing independent feedback and challenging participants' assumptions. This enables the organization to regularly and efficiently anticipate potential risks and adjust their business strategy.

Organizations routinely assess the potential impact of natural disasters on its operations and supporting infrastructure, enhancing its DR plans as required. While the first line of defense owns the DR plans, the second line facilitates periodic risk assessments and the third line assesses the effectiveness and testing of DR plans – this helps to ensure that potential risks are adequately reviewed and the organization is prepared should a catastrophe occur.

In each example, biases are eliminated due to the involvement of multiple parties enabling the organization to efficiently and effectively anticipate and limit the impact of potential risks.

78%

of respondents only prepare management dashboards annually or quarterly, indicating further opportunity exists to provide decision-makers with vital risk insights.

63%

of respondents have defined KPIs or KRIs, but not both. Fifty percent of respondents monitor KPIs, KRIs or both by leveraging technology.

61%

of respondents with defined KPIs and KRIs indicated they were using monitoring to identify trends or risks that may impact their organization's business strategy.

A robust risk-aware organization

Where are organizations now?

Over the last five years, organizations have improved the way they identify, manage and respond to risk. They have created executive-level roles to provide risk oversight, established functions to deal with complex legal and regulatory requirements, and implemented supporting technologies. Reacting to increased market volatility and regulatory changes, organizations renewed efforts to enhance their internal controls. While organizations have demonstrated progress, further opportunity exists to better manage risk and drive performance – **there is no reward without risk**.

Risk is a key part of strategic business planning and top of mind of many boards today; however, the board's ability to provide oversight could be enhanced by more frequent evaluations of the organization's risk profile.

88%

of respondents indicate that the board or a board committee provides oversight of the organization's risk management activities.

83%

of respondents identify, assess and develop plans to address risks to all key initiatives (43%) or identify and discuss the risks (40%).

77%

of respondents evaluate their organization's risk profile on an annual basis, limiting their ability to adjust their business strategy based on changes to their risk landscape.

Seizing the opportunity

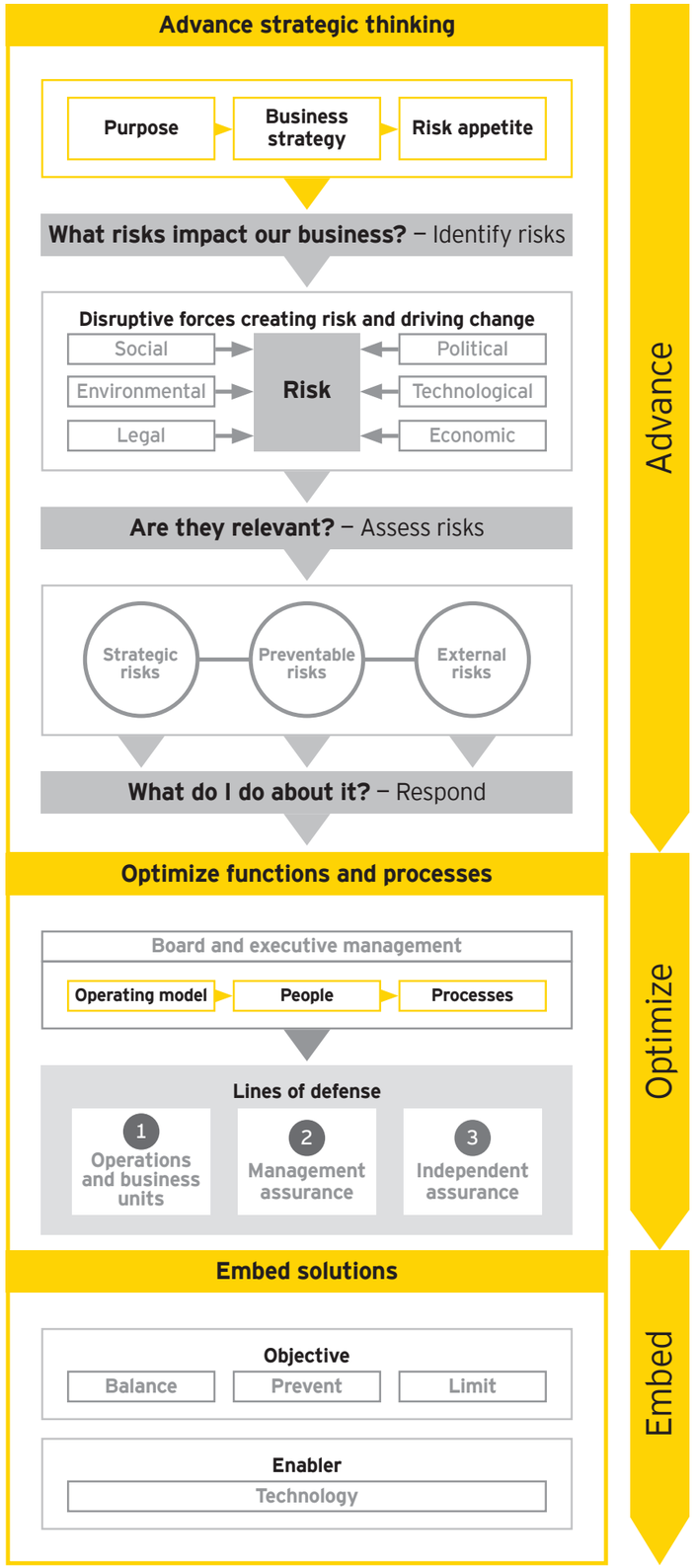
In summary, organizations exist to deliver on a purpose. That purpose is achieved through a series of business decisions that require taking risks – these risks impact business performance. Identifying, managing and responding to risk should be an integral part of an organization's everyday activities.

To drive performance, organizations must **advance** their strategic thinking. They need to identify and assess the risks that impact their business strategy. They also need to respond to those risks applying three categories – strategic, preventable and external. This enables organizations to shift their focus from the risks they can control to the ones they cannot or need to balance to drive performance.

To efficiently and effectively respond to risk, organizations must **optimize** their functions and processes. They need to define an operating model with clear ownership and accountability, align the right talent and skillsets to that operating model and design processes to govern the execution of risk activities. This establishes the structure and mechanisms to facilitate coordination, communication and reporting throughout the organization.

Once the functions and processes are properly in place, organizations can more easily **embed** and execute solutions that help them respond and manage risk as a core aspect of their business. These solutions, designed based on the three categories above, enable the organization to prevent, balance or limit the impact of risks. Leveraging enablers such as technology, organizations can support and sustain these solutions.

EY can help organizations think differently about risk so that they can manage the risks that drive performance and success.



"When we help clients approach their risk management in this way, they are able to set themselves more challenging goals that can deliver better outcomes."

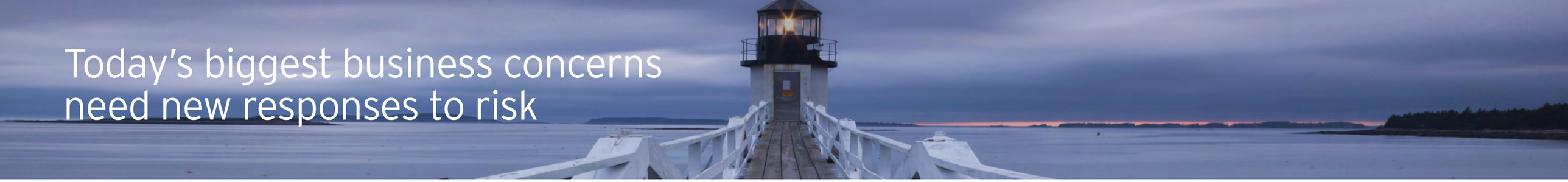
Paul van Kessel, Global Risk Leader

One business strategy: three different responses to risk

This example represents the actions a company that "thinks differently" about risk would apply. The response, impact and events are based on actual experiences with our clients.

A large consumer products company plans to make significant investments in social, mobile and digital platforms to improve its marketing and sales channels as well as its ability to bring products to market faster. Recognizing the importance of digital technology to its growth and brand, management is willing to accept a moderate level of risk. As part of developing their business plans, management identified several risks that could impact their investment in digital technology and developed three different responses to those risks.

	Strategic ROI is heavily dependent on bringing the platforms to market quickly to increase market share and brand awareness.	Preventable Legal and regulatory requirements governing digital marketing and sales channels (e.g.,Federal Communications Commission (FCC)) need to be addressed to avoid incurring fines or undergoing any regulatory scrutiny, especially given its desire to improve its brand recognition.	External Competitors are exploring similar digital platforms and avenues that could severely hinder efforts to enter the space.
Advance	▸ Management needs to act quickly, but does not intend to compromise quality or cost; they develop a plan to continuously review the project to make sure the expected benefits and ROI are realized.	▸ Management should implement controls to incorporate the new requirements into its existing risk and controls framework.	▸ Management needs to understand the potential impact of competitor actions and determine how to best limit it; they develop a strategy to conduct a series of "wargames" to assess and respond to potential moves by competitors.
Optimize	▸ Management tasks second and third lines of defense with reviewing the project at its initiation. ▸ Management identifies and embeds experts within the lines of defense to help predict potential risks prior to the start of the project. ▸ The second and third lines of defense will work with the first line to understand the project structure, governance and execution plan. In addition, the second line will work with the third line once the project starts to perform periodic assessments and benefits monitoring.	▸ Management tasks the second and third lines of defense with consulting and assessing the first line's changes to the company's internal controls. ▸ Lacking risk and compliance talent in this space, the company hires digital subject-matter resources within both lines to provide expertise and guidance.	▸ Management tasks its second line of defense with facilitating the exercises with participation from the first line. ▸ The third line is responsible for providing independent feedback and challenging the scenarios developed based on emerging trends. ▸ The resources selected to participate understand the business and have backgrounds in marketing and technology. They are to divide into smaller teams on a quarterly basis, develop viable competitor scenarios and report their findings to management.
Embed	▸ The second line of defense conducts interviews with the project team and leverages predictive analytics to identify potential risks. Several risks are identified with the project's execution and governance structure that would negatively impact the achievement of critical milestones. ▸ The second line works with the first line to take remediation steps. ▸ Going forward, the second and third lines work together to proactively identify risks before they arise, helping the company achieve its expected benefits under the desired timeline.	▸ The second line of defense works directly with the first to enhance the company's internal controls to address the new risks. However, rather than just increasing the complexity of the control environment, they optimize the controls framework by leveraging automated, preventive controls or controls that already exist. ▸ The third line helps assess the design and operating effectiveness of the controls before they are fully implemented. The internal control environment is updated to address the new requirements and optimized to prevent related risks.	▸ The combined team convenes quarterly and conducts wargames, identifying potential competitor actions. Each action is vetted and the most realistic are compiled by the second line of defense and shared with the executive management. ▸ Management reviews the team's findings adapting their strategy and level of investment as appropriate, helping to maximize their ROI.



Today's biggest business concerns need new responses to risk

A clear purpose drives results ...

Employees are three times more likely to stay with a purpose-driven company.*

Seventy two percent of global consumers would recommend a company with a purpose.*

As you start to think about your organization's opportunity to better manage risk, we wanted to highlight related topics that can help you in that endeavor based on our experience working with our clients.

Purpose-led transformation

Companies routinely state or imply their purpose through various mechanisms including promotional material, client proposals and public speaking forums. With these statements, they set an expectation with the public that they represent certain values, performance standards and service quality, to name a few. Failure to meet these expectations poses significant risk to the brand and reputation of a given organization.

From a risk management perspective, a company's ability to identify, measure and monitor strategic risk is the most direct link to their stated purpose. Proper mitigation of this strategic risk is the best means of ensuring realization of the ultimate purpose.

Performance-led transformation (PLT) offers an approach to realizing and activating a company's purpose – the "why" a company's products and services are aligned with the needs of their customer base. PLT helps organizations send a clear message to the market about what they stand for.

The benefits of injecting "purpose" into the fabric of a company's processes include:

- Improving execution and overall growth
- Creating a rallying point for company employees
- Driving new innovation
- Galvanizing company strategy
- Driving results

Purpose forces business leaders to manage and respond to the risks that matter most. When purpose is put at the forefront of all important business initiatives and decisions (i.e., "why" are we pursuing a certain path), it becomes clearer as to which risks may stand in the way. PLT helps organizations think about the risks that could prohibit the company from realizing its purpose as well as the achievement of its strategic business objectives.

For information about EY's Purpose-Led Transformation, please visit ey.com/PLT.

Approximately US$682b is wasted on underperforming projects across the globe annually.

Program risk management

Drivers such as innovation, technology shifts, evolving business models and regulatory change have forced companies to transform the way they operate and generate value. Successfully addressing the risks and challenges associated with transformation can create significant value for an organization – reduced project cost, reduced project time, increased benefit realization and improved time to benefits. However, strategic project execution continues to produce disappointing results.

Program risk management (PRM) allows organizations to unlock the value of their strategic programs; enabling them to deliver projects that support their business strategy and maximize the expected benefits. PRM helps with:

- Identifying programs that directly align with business objectives
- Prioritizing and balancing the program portfolio to maximize ROI
- Anticipating and limiting the impact of potential project risks
- Improving program execution and time to market
- Monitoring and driving benefits realization

Leading organizations apply portfolio management and predictive analytics to build confidence in successfully executing projects. They consider program risk as part of regularly assessing their risk landscape, they optimize functions and processes to best respond to identified risks, and, they embrace solutions that enable them to deliver successful programs.

The ability to have a forward-looking view of risks and being able to predict the impact of those risks allows the organization to proactively manage and balance their portfolio of projects. The key is to help executives identify projects with the best potential and then to enable them to nurture the most valuable and innovative programs: this requires having the right processes and tools in place to enable the early identification of risks. The ability to make adjustments to the project's governance, controls and processes prior to the onset of issues leads to greater control of program performance and accelerated benefits achievement.

For information regarding our EY's PRM service offerings and solutions, please visit ey.com/PRM.

Embracing a digital future

To many people it might feel like a digital future has already arrived, but the new technologies of today will look tame in comparison with the technologies that will emerge tomorrow. The Internet of Things (IoT) is becoming more active and more engaged as more and devices become connected – however, it is estimated that today only 1% of devices are currently connected. When more are online, it will have a profound impact on our personal, social and professional lives. It will be big business too: the wearable technology sector alone is expected to expand rapidly in the near future, with some experts forecasting growth of between US$10bn and US$50bn in the next five years.

It is now widely accepted that the four areas of digital change that will have the greatest impact on businesses are: cloud computing, data, social media and mobile technology, and each introduces specific risks into the landscape. Yet, with each risk, there is always opportunity. To capitalize on the potential, businesses need to develop an ambitious digital strategy.

We believe there is a three-stage process to help organizations maximize the possibilities of digital innovation. The EY Digital Realization™ Framework focuses on these phases of the digital journey: create, incubate and activate.

For information about your digital landscape, please visit ey.com/digital.

Cybersecurity

The same advances in technology – especially the networks within the Internet of Things – that are transforming lives, are also creating vulnerabilities for data security and organizations of every kind need to keep themselves and their customers safe from cybercrime. Today's cybercriminals are sophisticated and conduct advanced and persistent attacks on organizations until their defenses are breached. Companies risk significant loss of physical assets, including data, as well as financial loss through lost revenues, and costly reputational damage. Cyberattacks can destroy organizations, and so must be considered a significant threat.

It is important that organizations not only maintain and enhance their traditional security controls, but continue to evolve their ability to rapidly detect and respond to threats. However, anticipating cyberattacks is the only real way to get ahead of cybercrime.

For information about getting ahead of cybercrime, please visit ey.com/cybersecurity, or see EY's latest Global Information Security Survey on ey.com/GISS.

Every opportunity created by digital technology also creates risk. Organizations need to understand and adequately address digital risk by performing targeted risk and program assessments, and implementing additional controls.

The question is not "if" your company will be breached, or even when? It has already happened. The real questions are: Is your organization aware of it, and how well are you protected for the future?

* *The Energy Project,* ***What Is Your Quality of Life at Work****, 2013. http://theenergyproject.com*

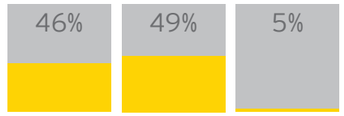
Survey findings

What our clients are telling us

In this year's GRC survey, we focused on an array of topics (e.g., risk strategy, coordination of functions, internal audit, technology) to gain a better understanding of how well organizations are managing risk today.

However, while organizations demonstrated they are making progress, they indicated that further opportunities exist to improve the way that they identify, manage and respond to risk.

Survey findings	Implications
Top five risks 1. Financial 2. Operational 3. Regulatory 4. Cybersecurity 5. Reputational **Bottom five risks** 1. Geopolitical crises 2. Natural disasters 3. Data privacy 4. R&D and product development 5. Mergers and acquisitions	▸ While organizations have expanded their view of risk, they continue to primarily focus on preventable risks. ▸ Organizations that also focus on strategic and external risks are able to profit from the upside of risk.
Link risk to the business  97% of organizations have made progress in linking their risk management objectives and business objectives ... ... but only 16% of the 97% consider them to be closely linked today.	▸ Organizations have made a significant amount of progress in bridging the gap between risk management objectives and business objectives. ▸ However, greater opportunity exists for organizations to achieve stronger alignment.
Risk involvement  66% of organizations indicated that risk management has limited involvement ... ... but 90% expect to be directly involved or providing inputs within the next three years.	▸ Organizations recognize the value of directly involving risk management in business decision-making. ▸ Organizations that directly involve risk management are better able to identify, manage and respond to the risks that impact their business.
Trends/risk drivers Challenges / Opportunities Cybersecurity: ■ / Reputation: ■ / ■ Strategic transactions: ■ / ■ Emerging markets: / ■ Economic stability: ■ / Technology shifts: / ■ Changing consumer preferences: / ■ Regulatory compliance: ■ /	▸ We are seeing businesses impacted by a multitude of disruptive forces and mega trends globally, each requiring a different response to manage the associated risk. ▸ Organizations are challenged with developing a comprehensive view of risk, as well as regularly identifying and responding to existing and emerging risks.
	▸ While a rapidly changing risk landscape creates challenges, it also presents opportunities. ▸ Organizations that manage risk well are better positioned to capitalize on the upside potential of risk.

Survey findings	Implications
Coordination of risk activities  21% of respondents indicated risk activities are well-coordinated today; whereas 67% indicated they expect risk activities to be well-coordinated within three years.	▸ Organizations expect to see a significant improvement in the level of coordination of risk activities. ▸ Companies must better align and coordinate risk activities throughout the entire organization to effectively and efficiently respond to risk.
Top internal audit skills or experience: 1. Critical/analytical thinking 2. Analytics 3. Risk management 4. Audit 5. Business strategy	▸ Businesses clearly recognize that their Internal Audit functions require the appropriate skills and experience to address the risks associated with a rapidly changing landscape. ▸ Organizations must appropriately develop and align talent with the requisite skill sets – not only in Internal Audit, but across each of their lines of defense.
GRC technology  46% of respondents do not yet utilize a GRC technology, 49% utilize one or more technologies and 5% did not know.	▸ We have witnessed many organizations adopt and leverage technology – in many cases multiple technologies – to better enable and sustain risk management activities. ▸ Organizations must view technology as a way to more efficiently and effectively execute, as well as sustain, their responses to risk.
GRC technology capabilities Medium / High Audit and compliance management: / ■ Policy management: ■ / Continuous monitoring: ■ / Security and process controls: / ■ Process improvement or automation: ■ / Document management: ■ / Data analytics and modeling: ■ / Dashboards and reporting: ■ / Enterprise risk management: / ■ Access to third-party content: ■ / Incident or issue management: ■ / Business continuity management: ■ /	▸ While organizations continue to prioritize capabilities typically associated with managing preventable risks, we are also seeing an increased demand for other capabilities (e.g., business continuity, data analytics and modeling, process improvement).

What we learned from the survey further validated our viewpoint that organizations need to think about, manage and respond to risk differently.

Internal Audit's evolving role

- Internal Audit is moving away from overseeing the risk management program to an assurance/advisory role that enables it to assess the effectiveness, efficiency and reliability of the organization's risk management program.
- As a result, Internal Audit can determine the extent to which it can leverage the work of others.
- This, in turn, can enable Internal Audit to adjust its scope to focus more of its efforts on the risks that matter, including strategic risks.

90% of respondents say risk management oversight is provided by someone other than Internal Audit.

46% of respondents say Internal Audit leverages the work of others today.

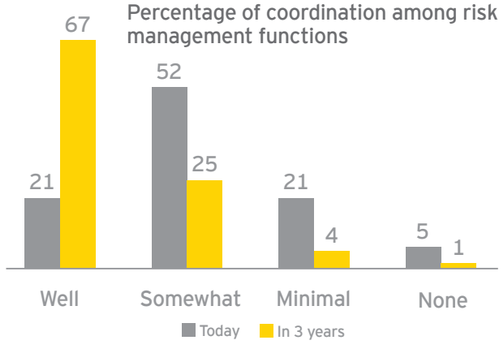
72% of respondents say Internal Audit will leverage the work of others in three years.

Top five opportunities for Internal Audit in 2015

1. Enhance ability to identify and assess emerging risks
2. Better leverage the work of other risk/control/compliance functions
3. Enhance reporting to present findings in perspective to the risks
4. Maximize usage of technology to reduce costs and improve risk coverage
5. Increase usage of data analytics

Optimizing functions and processes

Organizations need to establish a structure in which it can efficiently and effectively execute its risk strategy.



Risk management policies and processes are integral to:

- Influencing behaviors
- Coordinating activities
- Establishing communication protocols
- Facilitating risk reporting

Respondents identified the following as the most important skills or experiences required to enhance their risk functions:

1. Risk management
2. Business strategy
3. Critical/analytical thinking
4. Regulatory compliance
5. Process improvement

The appropriate operating model, talent, skillsets and risk management policies and processes enable the smooth execution of risk response activities.

Survey methodology

Our global governance, risk and compliance survey 2015 was conducted between February and March 2015: it asked how well organizations are managing risk and what they need to do to better manage the risks that drive performance. Almost 1,200 members of the C-suite, board audit committees and various assurance and/or compliance executives participated – representing major industries in 63 countries around the globe. The majority of the survey responses were collected during face-to-face meetings: when this was not possible, the questionnaire was completed online. We thank all participants for their invaluable insights.

Profile of participants

1,196 respondents

63 countries worldwide

25 industry sectors

Respondents by industry sector

Automotive and transportation	77
Banking and capital market	146
Cleantech	4
Consumer products	121
Government and public sector	72
Health care	46
Insurance	49
Life sciences	32
Media and entertainment	29
Mining and metals	46
Oil and gas	53
Power and utilities	90
Real estate	21
Technology	73
Telecommunications	48
Wealth and asset management	20
Other (please specify)	269

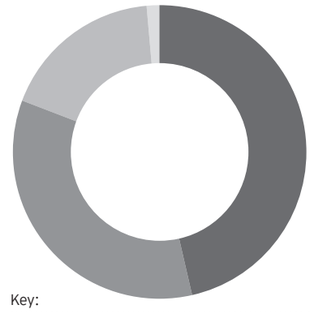
Respondents by number of employees

Less than 1,000	320
1,000 to 5,000	293
5,000 to 15,000	235
15,000 to 50,000	188
50,000 plus	160

Respondents by roles/titles

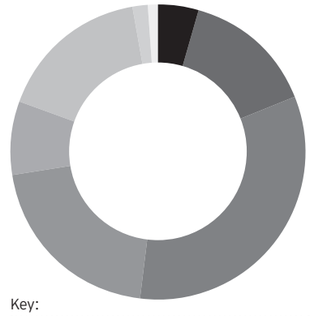
Board of directors member – audit committee member	15
Board of directors member – risk committee member	6
Chief executive officer or president	18
Chief financial officer (or equivalent)	62
Chief information officer	13
Chief risk officer	127
Chief audit executive	648
SOX/compliance leader	57
Other (please specify	250

Respondents by area



Key:	
EMEIA	556
Americas	411
Asia-Pacific	214
Japan	15

Respondents by total annual company revenue



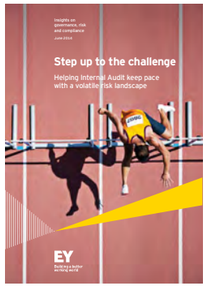
Key:	
More than US$50 billion	55
US$10 – US$50 billion	174
US$1billion – US$10 billion	393
US$100 million – US$1 billion	248
US$10million – US$100 million	95
Less than US$10 million	198
Government, nonprofit	21
Not applicable	12

Want to learn more?

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.

Maximizing value from your lines of defense

ey.com/LOD



Step up to the challenge: helping Internal Audit keep pace with a volatile risk landscape

ey.com/IArisks

Improve your business performance: transform your governance, risk and compliance program

ey.com/transformGRC

Get ahead of cybercrime: EY's Global Information Security Survey 2014

ey.com/GISS

Cyber program management: identifying ways to get ahead of cybercrime

ey.com/CPM

Megatrends 2015: making sense of a world in motion

ey.com/megatrends

Expecting more from risk management: drive business results through harnessing uncertainty

ey.com/REPM

Unlocking the value of your program investments: how predictive analytics can help in achieving successful outcomes

ey.com/PRM

Harnessing the power of data: how Internal Audit can embed data analytics and drive more value

ey.com/IAanalytics

If there's no reward without risk, can risk be a good thing?

Risk is a much more risky proposition than it used to be. New risks emerge every day as markets get disrupted, political instability interrupts supply chains and new technology pushes boundaries across the risk landscape. Yet, while many organizations see risk as a negative, good risk management can actually help companies go faster.

For EY Advisory, a better working world means solving big, complex industry issues and capitalizing on opportunities to deliver outcomes that help grow, optimize and protect our clients' businesses. We've shaped a global ecosystem of consultants, industry professionals and alliance partners with one focus in mind – you.

We help you make incremental strategic decisions around risk management to help your business strategy stay on course. We help you look at risk from all angles and across every part of the organization, including cybersecurity, supply chain, internal audit and risk assurance.

Our global connectivity and understanding of your issue inspire us to ask better questions. We then co-create more innovative answers that enable you to develop a top-down, risk-based approach to transforming your risk management environment. Together, we help you deliver better outcomes and long-lasting results, from strategy to execution.

We believe that when organizations manage risk better, the world works better.

So, if there's no reward without risk, can risk be a good thing? Ask EY.

The better the question. The better the answer. The better the world works.

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.

EYG no. AU3214

1503-1415327 EC
ED None.

ey.com/GRCinsights

About EY's Advisory Services

In a world of unprecedented change, EY Advisory believes a better working world means solving big, complex industry issues and capitalizing on opportunities to help deliver outcomes that grow, optimize and protect clients' businesses.

Through a collaborative, industry-focused approach, EY Advisory combines a wealth of consulting capabilities – strategy, customer, finance, IT, supply chain, people and organizational change, program management and risk – with a complete understanding of a client's most complex issues and opportunities, such as digital disruption, innovation, analytics, cybersecurity, risk and transformation. EY Advisory's high-performance teams also draw on the breadth of EY's Assurance, Tax and Transaction Advisory service professionals, as well as the organization's industry centers of excellence, to help clients deliver sustainable results.

True to EY's 150-year heritage in finance and risk, EY Advisory thinks about risk management when working on performance improvement, and performance improvement is top of mind when providing risk management services. EY Advisory also infuses analytics, cybersecurity and digital into every service offering.

EY Advisory's global connectivity, diversity and collaborative culture inspires its consultants to ask better questions. EY consultants develop trusted relationships with clients across the C-suite, functions and business unit leadership levels, from Fortune 100 multinationals to leading disruptive innovators. Together, EY works with clients to co-create more innovative answers that help their businesses work better.

The better the question. The better the answer. The better the world works.

With 40,000 consultants and industry professionals across more than 150 countries, we work with you to help address your most complex industry issues, from strategy to execution. To find out more about how 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**

Our Risk Advisory Leaders are:

Global Risk Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Global Internal Audit Leader		
Michael O'Leary	+1 585 987 4605	michael.oleary@ey.com
Global Risk Transformation Leader		
Matt Polak	+1 412 644 0407	matthew.polak@ey.com
Area Risk Leaders		
Americas		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
EMEIA		
Jonathan Blackmore	+971 4 312 9921	jonathan.blackmore@ae.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp