AberdeenGroup
A Harte-Hanks Company

Send to a Friend

Enterprise Risk Management: The Art of Avoiding Unpleasant Surprises

February 2009

Stephen Walker

Executive Summary

The two fundamental purposes of this report are first, to identify the strategies, high-level tactics, internal capabilities and frameworks, technologies, and services that top performing companies are employing to realize substantial business benefits from their Enterprise Risk Management (ERM) programs. Secondly, to provide a roadmap of actionable analysis and recommendations that both companies planning to develop an ERM program for the first time, and companies seeking to augment and optimize an existing initiative can leverage to improve their performance in assessing and managing risks strategically across the enterprise.

Research Benchmark

Aberdeen's Research Benchmarks provide an in-depth and comprehensive look into process, procedure, methodologies, and technologies with best practice identification and actionable recommendations

Best-in-Class Performance

Aberdeen used three key performance criteria to distinguish Best-in-Class companies. Best-in-Class companies achieved, on average:

- **21% increase** in management's visibility of the company's current risk status
- **17% increase** in the ability to provide clear, timely communication of risks to key stakeholders - including shareholders and the board of directors
- **15% increase** in the translation of collected risk assessment data into actionable business recommendations

Competitive Maturity Assessment

Survey results show that the firms enjoying Best-in-Class performance shared several common characteristics:

- Best-in-Class companies are more than 2.5-times as likely as Laggards to employ both qualitative and quantitative risk assessment processes
- Best-in-Class companies are 65% more likely than the Industry Average to use training programs for employees on relevant risk management issues and scenarios

Required Actions

In addition to the specific recommendations in Chapter Three of this report, to achieve Best-in-Class performance, companies must:

- Ensure executive-level commitment to the ERM initiative, characterized by upper management being actively involved in establishing and embedding the overall strategic direction of the company's risk management philosophy
- Establish a cross-functional team to develop, maintain, and standardize risk management policies and procedures across lines of business and geographies

"A large share of the blame for the financial markets and sub-prime crisis can be linked to the fact that regulators were too focused on institutions, not on the whole system of risks."

~ CEO, Small European-based Software Provider

Send to a Friend

Table of Contents

Figures

Tables

Chapter One: Benchmarking the Best-in-Class

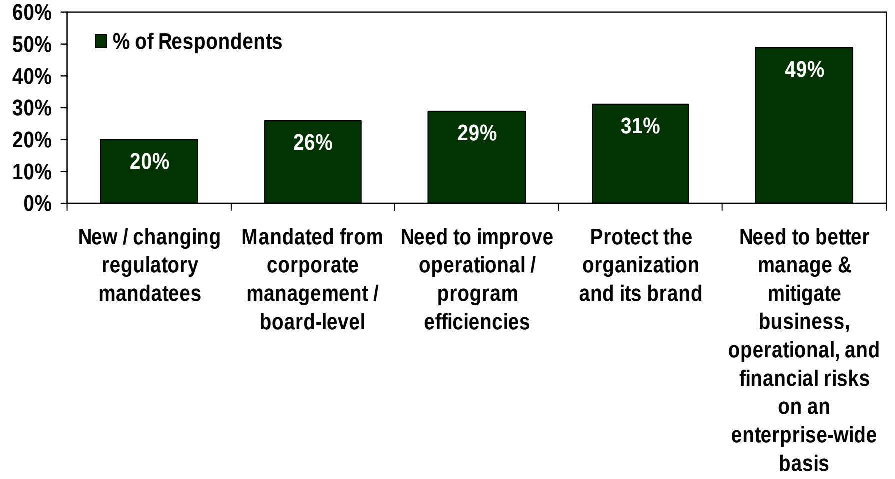
Business Context

Risk management is one of the fastest growing and heavily discussed segments of the technology and services market. Its popularity and growth is matched only by its demand. Most recently brought to the forefront of executive-level initiatives with the financial markets meltdown, the need for enterprise-spanning, effective, and efficient risk management procedures, controls, and solutions has never been greater.

Recent research from Aberdeen Group's upcoming May 2009 benchmark study, *Convergence and Integration: Risk and Compliance Strategies for FSIB*, reveals that the two areas organizations are most concerned with in 2009 (i.e. the areas organizations feel *least* confident about being able to effectively address) include managing risks across the enterprise (44%) and ensuring accurate and timely communication of risk and compliance status to key stakeholders (27%).

For many organizations, particularly those competing in multi-regulatory environments*, a significant amount of focus and resources in 2009 and beyond will be devoted towards strategies that minimize a loss event through concentrating on oversight, assurance, and enterprise-wide risk management. Currently, the top macro-economic business pressures driving organizations to invest resources in improving their performance in assessing and managing risks strategically across the enterprise is the need to better manage and mitigate business, operational, and financial risks on an enterprise-wide basis (Figure 1).

Figure 1: Top Pressures Driving Risk Management Investments



Source: Aberdeen Group, February 2009

Strategic Insight:

Given the across-the-board immaturity of currently employed ERM programs, combined with the potentially catastrophic magnitude of *not* having such a program in place, an eruption of activity in the ERM space has begun that spans industry, geography, and company size.

***Multi-regulatory Industries / Environments Defined:**

Such industries are required to achieve and prove compliance with a variety of governmental (including federal, state, and municipal) and industry-specific regulatory mandates. Such regulations are frequently amended or changed and differ, sometimes greatly, in terms of scope and applicability within an individual organization. Common examples of multi-regulatory industries include:

√ Banking / financial services / insurance

√ Pharmaceutical manufacturing

√ Energy and utilities

A Wake-up Call of Epic Proportions

Due to its highly prevalent and widely publicized use in Financial Service, Insurance, and Banking (FSIB) organizations, holistic and integrated risk management processes in general, and Enterprise Risk Management (ERM) in particular, were historically viewed by many organizations outside of FSIB as "sound's like a good idea in the future" at best. However, in the wake of the subprime mortgage crisis, ensuing instability in global financial markets, and the subsequent uncertain economic landscape, organizations have been struck by several disconcerting revelations resulting in a tremendous rise of discussion, activity, and investments in the ERM space:

1. That currently employed ERM practices, particularly in Financial Services, proved completely inadequate
2. The resulting across-the-board economic fall-out was substantially aided by ineffective, siloed risk management activities that failed to account for and preemptively manage systemic risk (how risks impact each other)
3. Standard and Poor's (S&P) announcement to introduce ERM analysis into the corporate credit ratings process globally for non-financial companies

Fueling the Demand for ERM

The importance of strategically addressing the expanding scope of business, operational, financial, regulatory, technology, and market risks inherent in today's global market is continually emphasized by media coverage of million and billion dollar losses associated with leaks of, and unauthorized access to, sensitive corporate, customer, and partner data and information. Yet despite the public nature of these risk management lapses, most companies are still very immature with respect to the tactics and processes employed to strategically manage risks on an enterprise level; less than 30% of surveyed companies have devoted resources towards ERM for over five years.

Given the across-the-board immaturity of currently employed ERM programs, combined with the potentially catastrophic magnitude of *not* having such a program in place, an eruption of activity in the ERM space has begun that spans industry, geography, and company size. Realizing the powerful and tangible connection between effective, comprehensive risk management and sustainable business growth, organizations are increasing both the amount and scope of budgetary investments in ERM solutions and services.

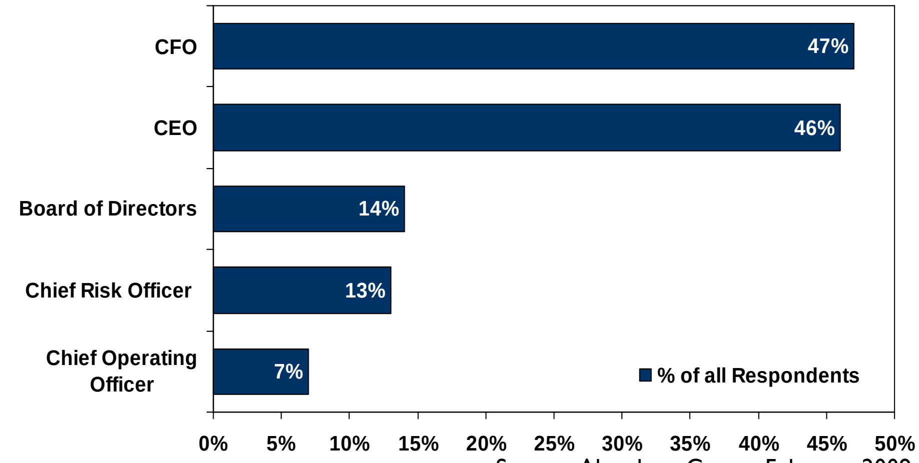
Overall, during the next fiscal year, companies reported double-digit budgetary investment increases in risk management evaluation and consulting services (11.2% increase over last fiscal year) and risk based tracking and reporting tools (13.4% increase over last fiscal year), with 10% of companies indicating that their budget's for ERM software platform's will rise by more than 30%.

Fast Facts

√ Best-in-Class companies are more than 1.75-times as likely as Laggards to have senior management actively involved with establishing and embedding the overall strategic direction of the company's risk management philosophy

In the same manner that budgetary allocations for enterprise-wide risk management investments are raising dramatically, so too has risk management budgetary decision-making responsibility elevated to the company's top executives (Figure 2).

Figure 2: Responsibility for ERM Investments



Source: Aberdeen Group, February 2009

The Maturity Class Framework

The value of any technology or service designed to help organizations assess and manage risks strategically across the enterprise is ultimately tied to the quantifiable results it delivers to the organization. Driving substantial and sustainable business-focused performance improvements through an enterprise-spanning risk management framework has been a challenge for the majority of organizations. Yet despite the across-the-board low maturity levels, Best-in-Class companies are realizing tangible benefits from their ERM activities. Aberdeen used three key performance criteria to distinguish Best-in-Class from Industry Average and Laggards organizations:

- Increase in management's ability to access the company's current risk status
- Increase in translating collected risk assessment data into actionable business recommendations
- Increase in the ability to provide clear, timely communication of risks to key stakeholders*

These Key Performance Indicators (KPIs) are the operational metrics most frequently touted by end-user organizations as being critical in determining the progress and success of an ERM initiative. Table 1 highlights the Best-in-Class performance in each of these metrics.

*Key Stakeholders:

For purposes of this report, key stakeholders include:

√ Shareholders

√ Boards of Directors

√ Senior Management

Table 1: Top Performers Earn Best-in-Class Status

Definition of Maturity Class	Mean Class Performance
Best-in-Class: Top 20% of aggregate performance scorers	▪ 20% increase in management's ability to access company's current risk status ▪ 17% increase in clear, timely communication of risks to key stakeholders ▪ 13% increase in translating collected risk assessment data into actionable business recommendations
Industry Average: Middle 50% of aggregate performance scorers	▪ 3% increase in management's ability to access company's current risk status ▪ 3% increase in clear, timely communication of risks to key stakeholders ▪ 2% increase in translating collected risk assessment data into actionable business recommendations
Laggard: Bottom 30% of aggregate performance scorers	▪ 1% increase in management's ability to access company's current risk status ▪ 2% increase in clear, timely communication of risks to key stakeholders ▪ 1% increase in translating collected risk assessment data into actionable business recommendations

Source: Aberdeen Group, February 2009

The Best-in-Class PACE Model

Achieving the Best-in-Class performance improvements in Table 1 requires a combination of strategic actions, organizational capabilities, and enabling technologies and services (Table 2).

Table 2: The Best-in-Class PACE Framework

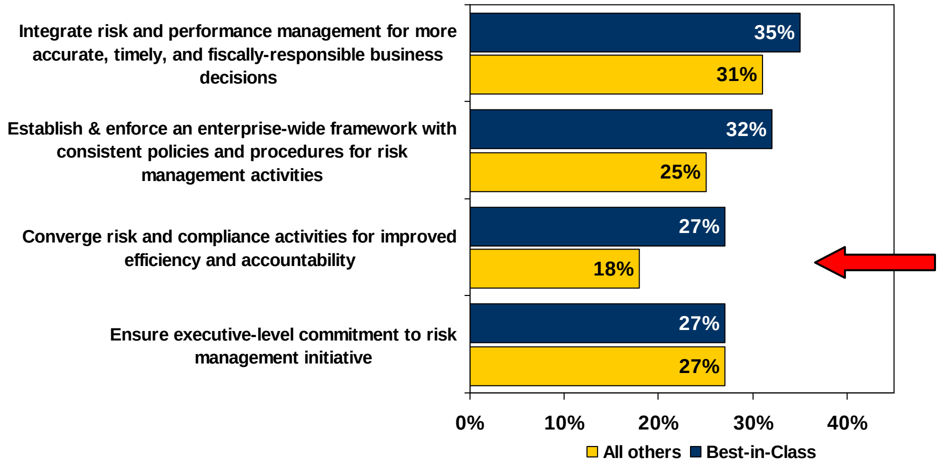
Pressures	Actions	Capabilities	Enablers
▪ Need to better manage and mitigate business, operational, and financial risks on an enterprise-wide basis	▪ Integrate risk and performance management for more accurate, timely, and fiscally-responsible business decisions ▪ Ensure executive-level commitment to risk management initiatives	▪ Processes that incorporate and mitigate risk exposures identified from both reactive and proactive procedures ▪ Qualitative and quantitative risk assessment processes in place ▪ Standardized risk-based responses for security events and incidents of non-compliance ▪ Senior management actively involved with establishing and embedding overall strategic direction of risk management philosophy	▪ Custom role / task based risk reports generated without help from IT staff ▪ Tools enabling visualization and communication of the interconnections and potential effects between risks across the enterprise ▪ Document and information management / workflow tools ▪ ERM platform / software ▪ Enterprise GRC platform / software

Source: Aberdeen Group, February 2009

Best-in-Class Strategies

Best-in-Class companies understand that a sustainable framework for consistent risk management performance improvements flows from an enterprise-wide approach that is consistent, repeatable, and measurable. Grasping that effective, business-advancing ERM is not a "check-box" / "every so often if we get around to it" activity. Best-in-Class companies employ strategic actions that emphasize operational efficiency, goal-oriented accountability, and the development of a risk-aware organizational culture that continually advances targeted corporate goals throughout the continuum of the ERM program (Figure 3).

Figure 3: Best-in-Class Actions to Improve ERM Performance



Source: Aberdeen Group, February, 2009

By establishing a cohesive framework of consistent, *not* rigid and identical, policies and procedures for risk management activities, the Best-in-Class establish a reliable baseline from which they can incorporate monitoring and measuring protocols and tools. In turn, this enables them to determine and integrate business-critical, or issue specific performance metrics that map back to and directly facilitate the advancement of current and future business goals.

The arrow in Figure 3 highlights that Best-in-Class companies are 50% more likely than all others to implement strategies to converge overlapping or synergistic portions of their risk management and compliance activities. The operational efficiencies gained from this approach are only available because a consistent, comprehensive, and measurable risk management framework is already in place. The primary reason only 18% of non Best-in-Class companies (representing 80% of surveyed organizations) identified this as a strategic action is due in large part to the fact that they are not ready to take that step. While it would be welcome to enjoy cost-saving operational efficiencies, most companies are still struggling to construct a risk framework that actually manages their risks.

"We have discussed [ERM] off an on, yet nothing has been formalized to manage it with control and direction."

~ Finance Manager, Large Middle Eastern-based Telecommunications Service Company

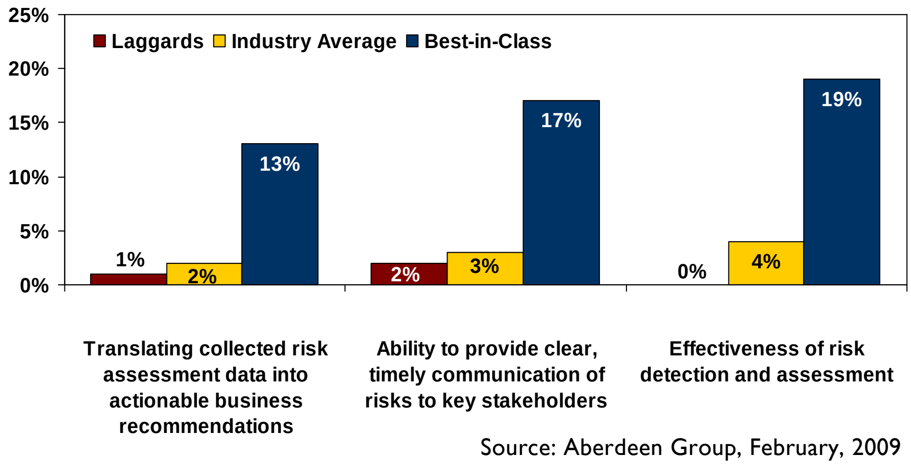
Best-in-Class companies understand that the end goal of an ERM program is the embedding of a risk-aware culture into the DNA of the organization, best characterized when risk management is incorporated into every-day business activities such that it is "something that is consistently being done" rather than "something else employees have to do." Focusing their strategic actions and budgetary allocations on developing and incorporating the internal capabilities, technologies, and services that facilitate this allowed Best-in-Class companies to improve the effectiveness of risk detection and assessment by 19%. As a result, they improved the translation of that collected risk assessment data into actionable business recommendations by 13%; an average increase more than five-times greater than the Industry Average. Particularly compelling when viewed from a C-suite perspective, these optimized risk management capabilities also enabled the Best-in-Class to improve their ability to clearly communicate a more accurate and timely view of the company's current risk status to key stakeholders (Figure 4).

Fast Facts

√ Best-in-Class companies are more than twice as likely as all other companies to have a central, secure, and accessible repository for all risk-related information

√ The Best-in-Class are 1.5-times more likely than all others to employ business leaders that actively work towards and advocate a culture of open risk communication

Figure 4: Best-in-Class Performance Improvements



Source: Aberdeen Group, February, 2009

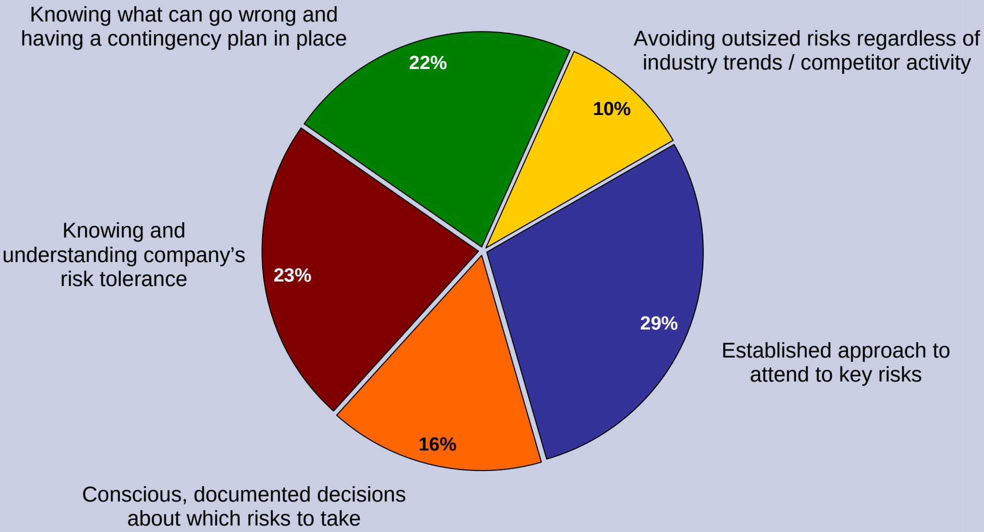
Aberdeen Insights — S&P ERM Strategies

The turbulence generated by Standard and Poor's (S&P) recent announcement to include ERM analysis into global credit rating evaluations for non-financial companies has publicly brought to light the previously ignored foundational chasm that exists in many risk management strategies; employee knowledge, buy-in, and active involvement with the ERM program. Reaffirming this notion, the area of their current risk management framework that companies feel *least* confident about being able to effectively address in 2009 is embedding a sustainable risk management culture into the organization. Specifically, out of the five generalized evaluation criteria S&P will be using, the two criteria that respondent companies will be devoting the most resources and investments to addressing and improving are an established approach to attend to key risks, and knowing and understanding the company's risk tolerance (Figure 5).

continued

Aberdeen Insights — S&P ERM Strategies

Figure 5: Expected Investments Devoted to S&P ERM Criteria



Source: Aberdeen Group, February, 2009

Our research confirms that at first glance some might dismiss the S&P ERM evaluation criteria. However, digging deeper into the overall market's immaturity with respect to ERM (particularly relevant to non-financial companies) the S&P announcement simultaneously: unearths a critical flaw existing in many of the risk strategies that companies are currently employing; while also offering forward-thinking companies a window of opportunity to use the announcement as a vehicle to drive organizational change.

Given the current global economic tightening, and the inherent difficulty in proving an ROI for effective risk management (it is almost always difficult to attach a dollar sign to something that *didn't* happen) a number of companies, across industries, have significantly cut or even frozen budgets for non-revenue generating business activities. Internal efforts to ensure the executive buy-in and budgetary allocations necessary to first establish, then build upon a comprehensive ERM program can be substantially aided through a two-pronged argument, essentially: 1) there a powerful business-driving, ROI-revealing value proposition flowing from effective ERM programs (although rarely is this realized right off the bat); and now 2) there is also a regulatory reason for addressing some of the foundational elements of an ERM framework. For companies without any real ERM framework in place, the "now we *have* to do it" element can be the impetus for cultivating a risk-based thought-process into the overall corporate mindset and leveraged as a spring-board to revamp ineffective, failed, or abandoned ERM programs.

In the next chapter, we will see what the top performers are doing to achieve these gains.

Chapter Two: Benchmarking Requirements for Success

The selection of technologies and services facilitating effective and efficient enterprise-spanning risk management, and integration with business intelligence, performance management, and business process management systems plays a crucial role in the ability to turn risk mitigation strategies into sustainable business performance advancements.

Case Study — Streamlining Risk Management

With 13,000 employees and annual revenues of roughly $5 billion, Spirit AeroSystems, the largest independent supplier of aerostructures to both Boeing and Airbus, needed to streamline, automate, and tie together the company's diverse compliance activities and render an accurate picture of constantly evolving enterprise risk across diverse business functions and geographies. Spirit Aerosystems' chief audit executive wanted a solution to manage the company's enterprise risk in a holistic sense. The challenges associated with this included addressing the variety of external (Sarbanes-Oxley, Federal Aviation Administration, and Environmental health and safety requirements to name a few) and internally mandated (a variety of comprehensive policies and procedures pertaining to the company's multi billion-dollar a year supply chain management function) compliance requirements. Compounding this problem, the solution needed to be implemented and usable in a tight time-frame with the IT department already in the middle of a large-scale technology implementation.

Needing a first-tier risk-assessment tool, easily configurable data collection functionality, and easy to use, flexible reporting features, Spirit AeroSystems' chose a comprehensive, hosted GRC solution. Three months after making the decision, the solution was up and running. Internal audit went live first, followed by the audit function for supply-chain management. Placing an emphasis on usability paid off handsomely; auditors used the solutions ad-hoc reporting tool to build what they needed without even going through training.

Spirit AeroSystems' cut the amount of resources devoted to SOX efforts by half, and internal audit teams across the globe now have access to the same files. "The efficiencies are incredible in terms of the time it takes us to complete an audit and get the documents reviewed and signed off – it's a very logical, quick process from start to finish in terms of auditing any particular area," Spirit Aerosystems' Chief Audit Executive said.

Moving forward, Spirit plans to move FAA and quality assurance-related compliance, environmental health & safety, and IT security onto the system. The end goal is to break down the legacy risk and compliance silos and provide a clear path to true enterprise risk management.

Competitive Assessment

Aberdeen Group analyzed the aggregated metrics of surveyed companies to determine whether their performance ranked as Best-in-Class, Industry

Fast Facts

√ As a direct result of their ERM programs, Best-in-Class companies were able to improve accuracy and timeliness of financial forecasting by 11%; an average increase more than 4.5-times greater than all others

Average, or Laggard. In addition to having common performance levels, each class also shared characteristics in five key categories: 1) **Process:** the approaches they take to execute their daily operations; 2) **Organization:** corporate focus and collaboration among stakeholders; 3) **Knowledge management:** contextualizing data and exposing it to key stakeholders; 4) **Technology:** the selection of appropriate tools and effective deployment of those tools; and 5) **Performance management:** the ability of the organization to measure their results to improve their business. These characteristics (identified in Table 3) serve as a guideline for best practices, and correlate directly with Best-in-Class performance across the key metrics.

Table 3: The Competitive Framework

	Best-in-Class	Average	Laggards
Process	Embedding processes that incorporate and mitigate risk exposures identified from both reactive (incident-based) and proactive (assessment-based) business procedures		
	87%	50%	24%
Organization	Cross-functional team to develop, maintain, and standardize risk management policies and procedures		
	60%	41%	10%
Knowledge	Senior management actively involved with establishing and embedding overall strategic direction of risk management philosophy		
	67%	53%	24%
	Routine communication of corporate objectives and company goals to risk management "teams" and process owners for consistent mapping back to established risk parameters		
	53%	38%	19%
Technology	Risk management technical capabilities currently in use:		
	▪ 60% complete and readily retrievable audit trail records to support analysis, internal and external audits, and documentation for reporting or investigation purposes ▪ 40% custom roll/task based risk reports generated without IT help ▪ 33% tools enabling visualization and communication of the interconnection and potential effects between risks across the enterprise	▪ 35% complete and readily retrievable audit trail records to support analysis, internal and external audits, and documentation for reporting or investigation purposes ▪ 35% custom roll/task based risk reports generated without IT help ▪ 24% tools enabling visualization and communication of the interconnection and potential effects between risks across the enterprise	▪ 24% complete and readily retrievable audit trail records to support analysis, internal and external audits, and documentation for reporting or investigation purposes ▪ 10% custom roll/task based risk reports generated without IT help ▪ 5% tools enabling visualization and communication of the interconnection and potential effects between risks across the enterprise

	Best-in-Class	Average	Laggards
Performance	Measurement / monitoring tools currently used to advance ERM initiative:		
	▪ 73% regular review of output from compliance management, auditing, and reporting solutions ▪ 58% consistent and frequent measuring of enterprise-wide risk status based on complete assessment of current risks ▪ 53% self-audit metrics for each business unit to measure risk management activity / progress against established milestones	▪ 41% regular review of output from compliance management, auditing, and reporting solutions ▪ 33% consistent and frequent measuring of enterprise-wide risk status based on complete assessment of current risks ▪ 41% self-audit metrics for each business unit to measure risk management activity / progress against established milestones	▪ 19% regular review of output from compliance management, auditing, and reporting solutions ▪ 19% consistent and frequent measuring of enterprise-wide risk status based on complete assessment of current risks ▪ 5% self-audit metrics for each business unit to measure risk management activity / progress against established milestones

Source: Aberdeen Group, February 2009

Capabilities and Enablers

Based on the findings of the Competitive Framework and interviews with end users, Aberdeen's analysis of the Best-in-Class reveals that there are a number of essential ingredients that advance the development of a sustainable, highly-communicative enterprise-wide risk management infrastructure. However, fully capitalizing on the brand-protecting, business-advancing benefits that flow from effective, proactively operationalized ERM programs requires the right blend of process, organizational, and knowledge management capabilities, as well as technology and service enablers.

Process

Best-in-Class companies are **more than twice as likely** as Laggards to establish and enforce consistent risk management policies and procedures across geographies and lines of business. Putting a consistent, yet flexible, framework of policies into place directly facilitates the establishment of a common risk-based language that accomplishes at least two critical objectives.

At the onset of the ERM program, this capability is invaluable in the identification, assessment, and prioritization of business-relevant risks. It is extremely difficult, and in most cases with large, dispersed companies, all but impossible to comprehensively address risks on a piece-meal, siloed basis. Business-critical risks are frequently mis-prioritized as unimportant because they are referenced in risk assessment reports by a variety of divergent labels.

Secondly, as the ERM program matures, companies can begin to identify redundant and outright unnecessary processes. This enables organizations to consistently re-prioritize their resources and devote them to the risks that have the largest potential impact on both their core business processes and highest-priority corporate objectives. Establishing an enterprise-spanning consistent framework for risk management activities allowed the Best-in-Class to experience a 19% increase in the effectiveness of risk detection and assessment, and a 9% increase in the elimination of redundant risk management activities and processes; an average increase more than 3.75-times greater than all other organizations.

Fast Facts

√ Best-in-Class companies are 50% more likely than all others to implement strategies to converge overlapping or synergistic portions of their risk management and compliance activities.

Case Study — A Risk-Based Approach to Efficiency

A US based pharmaceutical company, with net sales of over $200 million, was preparing for a pending IPO. Given the importance of the event, the company's management team, Board of Directors, and internal audit department were focused on creating a top-down, risk-based, internal controls program that followed the AS5 and SEC interpretive releases. At the time the company was relying on MS Excel and Word to document its processes and controls; a common, but fragmented approach with troubling issues around both version control and ownership. In concert with outside consultants, the internal audit team had identified over 600 key controls for a centralized location with no subsidiaries or divisions.

The company's primary goal was to install a GRC system that adopted associated risk management processes while minimizing the use of internal IT resources. Their secondary goal was to have the system quickly adopted by external auditors. To achieve these goals, the pharmaceutical company decided on a GRC platform solution delivered as an on-demand Software-as-a-Service (SaaS) product.

The SaaS based solution allowed the company to easily train process owners, transfer that process ownership to impacted areas, and reduce the amount of outside resources. Working closely with the solution provider, the company first consolidated the data into a single repository to establish a consistent approach across the organization. Then, using the solutions embedded Internal Control over Financial Reporting (ICFR) methodology; the internal audit team identified the "correct" number of key controls, reducing the count from over 600 to 230, enabling an estimated savings of $250k. This also allowed internal audit to define the timing, nature, and extent of testing ensuring relevant, descriptive, and adequate testing coverage resulting in estimated savings of an additional $150k.

continued

Case Study — A Risk-Based Approach to Efficiency

Less tangible but still vital, external auditors, recognizing the seamless integration and reliability of the solution, readily approved the new framework and testing plan. Additionally, the internal IT resources that were formerly devoted to these activities were able to be refocused on strategic sales and marketing initiatives. "With [the solutions] on-demand model, there were no internal IT resources needed and it installed quickly and easily in a matter of days. Training was a snap; it was easy to share with process owners, external auditors, senior management and Board members," said the executive director of internal audit at the pharmaceutical company.

Organization

The Best-in-Class are twice as likely as all other companies to have a central, secure, and accessible repository for all risk-related information. Additionally, they are **1.5-times more likely** to have business leaders that actively work towards and advocate a culture of open risk communication. While the end goal of an ERM program is to *proactively* identify, manage, and plan for risks that would detrimentally affect the business before they do, developing a risk information repository can prove invaluable, particularly for companies with immature or non-existent ERM programs. For example, while the memory of a given employee is fleeting, cultivating this organizational capability can help to place the organization's collective memory on a continuum that helps to ensure companies are not unnecessarily hamstrung by repeating the same mistakes made in the past.

Especially valuable when leveraged through an organizational culture of open risk communication, regular discussions / reviews of historic risk information can serve as the spark that ignites a highly communicative, full-circle, and continuously employed strategy adjustment cycle. Here, previously successful (or, for that matter, unsuccessful) strategies can be analyzed, re-structured, and updated to address the ever-changing spectrum of risks.

By promoting a work environment that encourages and rewards risk-centric ideas and discussions while facilitating a forum that consistently collects, tweaks, and re-focuses risk strategies, the Best-in-Class were able to increase the detection of weaknesses in internal risk management processes and controls by 10%, and improve their ability to adjust those processes and controls to changes in regulatory requirements and business demands by 11%; an **average increase ten-fold higher than Laggards**.

Knowledge Management

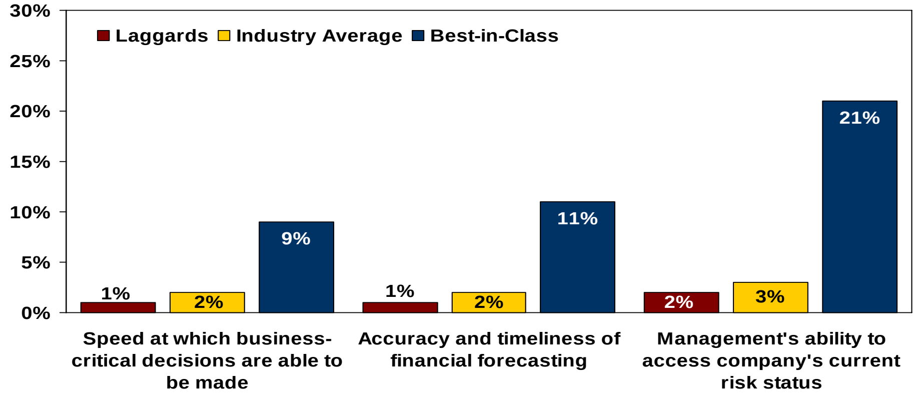
Best-in-Class companies are **more than 1.75-times as likely** as Laggards to have senior management actively involved with establishing and embedding the overall strategic direction of the company's risk management philosophy. As outlined at the end of Chapter One (in both the Best-in-

Class Strategies section and subsequent Aberdeen Insight box) one of the most important developmental areas, and one of the most difficult hurdles to overcome on the path to effective ERM, involves the organizational transition away from the prevailing ad-hoc, "check-list" view of risk management, and towards an deeply ingrained risk-based mindset about day-to-day business activities.

Best-in-Class companies are more than twice as likely as Laggards to task a responsible executive with primary ownership of the ERM program. Although merely positioning the overall ownership of the ERM program high in the organizational structure does not ensure its acceptance and use, Best-in-Class strategies go well beyond the "appearance of ERM for appearance's sake" epidemic plaguing a significant number of companies in today's market. Acting as a conduit between the executive team and the risk-tasked employees, the executive can enable full-circle communication characterized by affected employees knowing and proactively working towards the achievement of critical business goals.

In addition to being able to take a top-down look at the current organizational structure and identify where tweaks and adjustments need to be made to establish the required communication channels, protocols, and decision-making hierarchies, the executive has the wherewithal to make these changes happen. This degree of senior-level involvement also assists upper-level decision-makers who can more efficiently focus and adjust current decisions and future engagements based on an enhanced understanding of how these activities affect corporate goals and predetermined risk thresholds. By focusing on developing risk-intelligent management capabilities, the Best-in-Class realized dramatic improvements in visibility, financial forecasting, and time-to-decision (Figure 6).

Figure 6: Visibility, Financial Forecasting and Time-to-Decision Gain



Source: Aberdeen Group, February, 2009

Technology

Best-in-Class companies are **more than twice as likely** as Laggards to incorporate analytics and tools to monitor risk-based KPIs on the achievement of enterprise-wide objectives. The Best-in-Class are also1.5-

times more likely to employ technologies that facilitate complete and readily retrievable audit trail records. These records are critical to support analysis, internal and external audits, and serve as documentation for reporting requirements and investigation / litigation purposes.

As regulatory requirements pertaining to ERM programs continue to expand in both scope and applicability, incorporating these types of technologies can significantly help companies to bridge the gap between *saying* they have an ERM program and *proving* they have an ERM program. Incorporating these types of technologies allowed the Best-in-Class to improve their documentation to show / prove to regulators and ratings agencies the level of sophistication and maturity of their ERM program by 13%; an average improvement tenfold greater than all other companies.

"We've put some applications in place, but risk management has been viewed as a 'have-to-do-it' not as a core business activity."

~ Risk Manager, Mid-size South African Mining Company

Performance Management

Best-in-Class companies are **1.8-times as likely as Laggards** to employ consistent process prioritization assessments to ensure that the most business-relevant risk management processes are monitored most frequently. In addition, they are more than nine-times as likely to use self-audit metrics for each business unit to measure risk management activity / progress against established milestones. At the onset, incorporating these capabilities allows for the establishment of "current operation" risk-centric performance baselines that, when supplemented with the right blend of analytic-backed technologies, provides companies with the opportunity to:

- Adjust corporate activities and strategies to ensure that pre-determined thresholds remain intact
- Escalate the identification, prioritization, and remediation of problem areas
- Track improvements in risk management functions by mapping current performance against the established baselines to validate ongoing budgetary allocations

Aberdeen Insights — Technology

Many organizations, especially those that are large, multi-national, or operating out of several or more disparate geographic locations, are not even aware of the potential risks that could impact their business. As the number of organizational and geographical "silos" for risk and compliance information and analysis grows (Aberdeen's February 2007 report, *GRC Strategic Agenda: The Value Proposition of Governance, Risk management, and Compliance*, revealed that only 15% of organizations responded that the number of these silos decreased over the past 12 months), it is virtually impossible for in-house staff to properly manage risks on an enterprise-wide perspective with a homegrown solution or on a disjointed basis. Another major disadvantage of operating in silos is that oftentimes there is no common language; the same risk can be phrased differently resulting in redundant, costly, and unnecessary mitigation.

continued

Aberdeen Insights — Technology

Without convergence and integration of risk processes and controls, there is no common framework to identify, prioritize, and communicate these risks through the necessary channels. Further compounding the problem, some of the silo operators don't want it to change.

In addition to placing a heavy focus on establishing and enforcing consistent risk management policies and procedures across geographies, lines of business, and functional areas, Best-in-Class companies are incorporating technologies that standardize actions taken in response to commonly occurring events. It makes neither dollars nor sense to have a number of different responses and reporting processes for the same or very similar events simply because they happen to occur across several different functional areas. By incorporating technical capabilities that allow for a standardized, risk-based response to commonly-occurring security events and incidents of non-compliance, in tandem with standardized reporting procedures supported by clear hierarchical accountability for risk management activities enable the Best-in-Class to realize the productivity and efficiency gains that flow from a common, repeatable approach to every-day risk-related activities.

Chapter Three: Required Actions

Whether a company is trying to move its performance in assessing and managing risks strategically across the enterprise from Laggard to Industry Average, or Industry Average to Best-in-Class, the following actions will help spur the necessary performance improvements:

Fast Facts

√ Best-in-Class companies improved their effectiveness of risk detection and assessment by 19%, while also improving the accuracy and timeliness of financial forecasting by 11%

Laggard Steps to Success

- **Distribute established risk management policies, practices, and thresholds to employees on an enterprise-wide basis.** Currently, only 14% of Laggards do this, as opposed to 64% of Best-in-Class companies. As soon as the relevant details about these items have been finalized, distributing them to all employees, regardless of job function, should be a top priority. Not only does it serve as additional documentation to provide to regulators and ratings agencies, more importantly, it solidifies the importance of the ERM program in the collective organizational thought process. The enterprise-wide distribution of the company's risk management policies, practices, and thresholds, more so even than the actual content of these items, helps facilitate the risk-based organizational culture that serves as the lynchpin in effective ERM programs.
- **Immediately incorporate a central, secure, and accessible repository for risk-related information.** While 65% of Laggards plan on establishing such a repository within the next 12 to 24 months, currently only 4% have done so. Establishing a risk-information repository can be used as one of the foundational building blocks to help drive a risk-centric mentality into employees at all levels. This is a good example of a tangible action, producing a tangible result that companies can use as a progress milestone on the intangible journey towards the organizational mind-set change that top performing ERM companies have enabled.

Industry Average Steps to Success

- **Make sure senior management is actively involved with establishing and embedding the overall strategic direction of the company's risk management philosophy.** Although 35% of the Industry Average plan on developing this capability, currently just over half (53%) are doing this. Organizational buy-in from the day-to-day business and process owners who will ultimately determine the success of the ERM program can be dramatically advanced or mortally wounded by the noticeable presence or absence of top-down commitment to the project. Organizational buy-in is critical to not only aligning the different levels and departments within a company, but also in realizing the goals of the overall initiative. Technology alone may, for a time, treat some of the symptoms, but cannot cure the illness.

- **Routinely communicate corporate objectives and company business goals to risk "teams" and process owners for consistent mapping back to established risk parameters.** Although 42% of Industry Average companies plan on incorporating this capability, currently less than half do so. Ineffectively communicating strategic corporate goals to daily business owners is a common problem in small and mid-size companies, and is even more prevalent in large companies. Ensuring this type of consistent communication helps to focus and prioritize risk management activities on the most business-critical, and fiscally relevant. Additionally, by mapping these back to the company's established risk parameters, upper-level decision makers significantly decrease the chance that a decision made, or engagement entered into, will expose the company to an unacceptable level of risk.

Best-in-Class Steps to Success

- **Accelerate the incorporation of additional Business Intelligence (BI) analytics and tools to monitor KPIs and Key Risk Indicators (KRIs).** Although the Best-in-Class are more than twice as likely as Laggards to have these technologies in place, less than 50% currently do. With the consistently multiplying amount and type of data is collected for analysis, intelligence tools can prove invaluable to risk management efforts. Reminiscent of the old west tradition of "panning for gold," these technologies help sift through the mountainous volumes of collected data and information to glean the important and relevant from the useless and unnecessary. Especially valuable when mapped back to corporate objectives and overall business goals, companies are increasingly finding value in incorporating analytic tools like dashboards to relay the pertinent knowledge to the individual who can capitalize on its availability.

Aberdeen Insights — Summary

Risk management is based on the premise that through an effective framework backed by the right solutions, organizations can analyze, identify, and thus manage and mitigate risk proactively. At a basic level it ensures that potential risks are dealt with before they develop into high-dollar problems. For companies unsure how to approach putting an ERM framework in place, two key factors to consider include:

- **Develop a clear picture of the current problems facing your organization and potential stumbling blocks in the future.** This is a critical step to avoid costly and repetitive quick-fix solution deployments.

continued

Aberdeen Insights — Summary

To understand how a ERM or GRC initiative can alleviate current and future problems while advancing business goals, the organizations must first have a deep understanding of what those problems are. Although a truly effective enterprise-wide initiative becomes part of the entire organizational structure itself, prioritizing current and future problems by timing and scope allows organizations to direct the proper focus on immediate risks.

- **Evaluate the current state of your organizations internal capabilities and structure.** The "G" in GRC is often the most difficult. By evaluating your organizations current capabilities and structure, you can develop an organizational framework that can fully support your GRC initiative. Education and training are particularly helpful here. Knowing employees will be responsible for the various aspects of the initiative, and properly training them on the required processes, controls, and information flows can save a tremendous amount of time, money, and headaches. A good governance framework incorporates training, continual monitoring, sufficient processes and controls, and clearly delineated roles and responsibilities. A great governance framework incorporates everything already mentioned, but is built on a foundation of company-wide knowledge understanding, and belief that each employee has a stake in advancing the goals of the business.

For companies with a solid organizational structure seeking to put an ERM program in place for the first time, and for those companies looking to optimize an existing ERM program, some of the features of a potential solution that are vital to effectively advance business goals and efficiently manage risks on an enterprise-wide level include:

- **Scalability**. Ensuring the solution can expand across various segments as the organization grows while adapting to future goals and needs.
- **Consistency**. Viewing the entire spectrum of risks from a consistent, repeatable approach allow for objective assessment, prioritization, evaluation, and management of those risks in a comprehensive manner that significantly reduces the costs suffered from redundant activities.
- **Visibility**. Having visibility into how risks are managed helps eliminate wasted time and money stemming from process owners not understanding the methods their counter-parts are employing to mitigate risks they both face and allows upper-management to be kept fully informed of the organization's current risk status and map it back to pre-determined risk tolerance levels to make the most informed business decisions.

Appendix A: Research Methodology

Between January and February 2009, Aberdeen examined the use, the experiences, and the intentions of more than 120 enterprises devoting resources to improving their performance in assessing and managing risks strategically across the enterprise in a diverse set of industries and geographies.

Aberdeen supplemented this online survey effort with interviews with select survey respondents, gathering additional information on ERM strategies, experiences, and results.

Responding enterprises included the following:

- *Job title / function:* The research sample included respondents with the following job titles: Risk, Compliance, and Audit Manager (16%); Director of Operations and Procurement (15%); EVP / SVP of Finance (8%); CTO and IT staff (13%); senior management (20%).
- *Industry:* The research sample included respondents from a variety of industries including: aerospace / defense (7%); banking (8%); industrial & general manufacturing (11%); oil and gas (6%); and pharmaceutical manufacturing (5%).
- *Geography:* The majority of respondents (59%) were from North America. Remaining respondents were from Europe (23%), the Asia-Pacific region (11%), and the Middle East / Africa region (7%).
- *Company size:* Forty-three percent (43%) of respondents were from large enterprises (annual revenues above US $1 billion); 34% were from midsize enterprises (annual revenues between $50 million and $1 billion); and 23% of respondents were from small businesses (annual revenues of $50 million or less).
- *Headcount:* Twenty-seven percent (27%) of respondents were from small enterprises (headcount between 1 and 250 employees); 23% were from midsize enterprises (headcount between 250 and 2,500 employees); and 48% of respondents were from large businesses (headcount greater than 2,500 employees).

Solution providers recognized as sponsors were solicited after the fact and had no substantive influence on the direction of this report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to readers at no charge.

Study Focus

Responding executives completed an online survey that included questions designed to determine the following:

√ The degree to which risk management technologies and services are deployed in their operations and the financial implications of their use

√ The structure and effectiveness of existing risk management frameworks

√ Current and planned use of risk management capabilities to aid operational and financial activities

√ The benefits, if any, that have been derived from enterprise risk management initiatives

The study aimed to identify emerging best practices for identifying, assessing, and managing risks, and to provide a framework by which readers could assess their own management capabilities.

Table 4: The PACE Framework Key

Overview

Aberdeen applies a methodology to benchmark research that evaluates the business pressures, actions, capabilities, and enablers (PACE) that indicate corporate behavior in specific business processes. These terms are defined as follows:

Pressures — external forces that impact an organization's market position, competitiveness, or business operations (e.g., economic, political and regulatory, technology, changing customer preferences, competitive)

Actions — the strategic approaches that an organization takes in response to industry pressures (e.g., align the corporate business model to leverage industry opportunities, such as product / service strategy, target markets, financial strategy, go-to-market, and sales strategy)

Capabilities — the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products / services, ecosystem partners, financing)

Enablers — the key functionality of technology solutions required to support the organization's enabling business practices (e.g., development platform, applications, network connectivity, user interface, training and support, partner interfaces, data cleansing, and management)

Source: Aberdeen Group, February 2009

Table 5: The Competitive Framework Key

Overview

The Aberdeen Competitive Framework defines enterprises as falling into one of the following three levels of practices and performance:

Best-in-Class (20%) — Practices that are the best currently being employed and are significantly superior to the Industry Average, and result in the top industry performance.

Industry Average (50%) — Practices that represent the average or norm, and result in average industry performance.

Laggards (30%) — Practices that are significantly behind the average of the industry, and result in below average performance.

In the following categories:

Process — What is the scope of process standardization? What is the efficiency and effectiveness of this process?

Organization — How is your company currently organized to manage and optimize this particular process?

Knowledge — What visibility do you have into key data and intelligence required to manage this process?

Technology — What level of automation have you used to support this process? How is this automation integrated and aligned?

Performance — What do you measure? How frequently? What's your actual performance?

Source: Aberdeen Group, February 2009

Table 6: The Relationship Between PACE and the Competitive Framework

PACE and the Competitive Framework – How They Interact

Aberdeen research indicates that companies that identify the most influential pressures and take the most transformational and effective actions are most likely to achieve superior performance. The level of competitive performance that a company achieves is strongly determined by the PACE choices that they make and how well they execute those decisions.

Source: Aberdeen Group, February 2009

Appendix B:
Related Aberdeen Research

Related Aberdeen research that forms a companion or reference to this report include:

- Continuously Compliant: Ensuring Proactive, Comprehensive Compliance; September, 2008
- Is Your GRC Strategy Intelligent? Analytics for Accurate Real-Time Visibility and Decision Making; July, 2008
- GRC Strategic Agenda: The Value Proposition of Governance, Risk, and Compliance; February, 2008
- GRC for Mobility: Are Enterprises Prepared for the Tipping Point?; April, 2008

Information on these and any other Aberdeen publications can be found at www.Aberdeen.com.

Author: Stephen M. Walker II, Esq., GRC Specialist, Governance, Risk management, and Compliance Practice, stephen.walker@aberdeen.com

Since 1988, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.2 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen plays a key role of putting content in context for the global direct and targeted marketing company. Aberdeen's analytical and independent view of the "customer optimization" process of Harte-Hanks (Information – Opportunity – Insight – Engagement – Interaction) extends the client value and accentuates the strategic role Harte-Hanks brings to the market. For additional information, visit Aberdeen http://www.aberdeen.com or call (617) 723-7890, or to learn more about Harte-Hanks, call (800) 456-9748 or go to http://www.harte-hanks.com