Galvanize
is now ◆ Diligent

7 steps to
performance-enhancing
ERM

Table of contents

Defining ERM

First, what is enterprise risk management (ERM)?

The Risk Management Society defines it as:

…a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.

ERM represents a significant evolution beyond previous approaches to risk management because it:
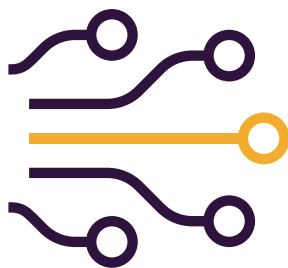
+ Encompasses all areas of organizational exposure to risk (financial, operational, reporting, compliance, etc.)

+ Prioritizes and manages those exposures as an interrelated risk portfolio, rather than as individual silos

+ Evaluates the risk portfolio in the context of all significant internal and external environments, systems, circumstances and stakeholders

+ Recognizes that individual risks across the organization are interrelated, and that they can create a combined exposure that differs from the sum of the individual risks

+ Provides a structured process for the management of all risks, whether those risks are primarily quantitative or qualitative in nature

+ Views the effective management of risk as a competitive advantage

+ Seeks to embed risk management as a component in all critical decisions throughout the organization

Characteristics of successful ERM

The most successful, high-performing organizations have ERM processes that share the following characteristics:

+ **Driven by data.** Built on the facts of what is actually taking place, by accessing and blending data in unique ways to identify risk trends and indicators.

+ **Dynamic.** Responsive to ever-changing risks and related events.

+ **Continuous.** Provides constant and timely insights in real time.

+ **Comprehensive.** Considers all aspects of all forms of risks, and their impacts on each other, and in aggregate.

+ **Collaborative.** Ensures that the three lines of defense are working in an aligned way around their respective responsibilities.

+ **Forward-looking.** Provides notifications of what is happening, what is likely to occur and what must be done in response.

+ **Contextual.** Provides insights that are relevant to managers at different levels and functions, and that align with overall corporate objectives.

+ **Highly efficient.** Driven by technology that is designed specifically for achieving all of the above.
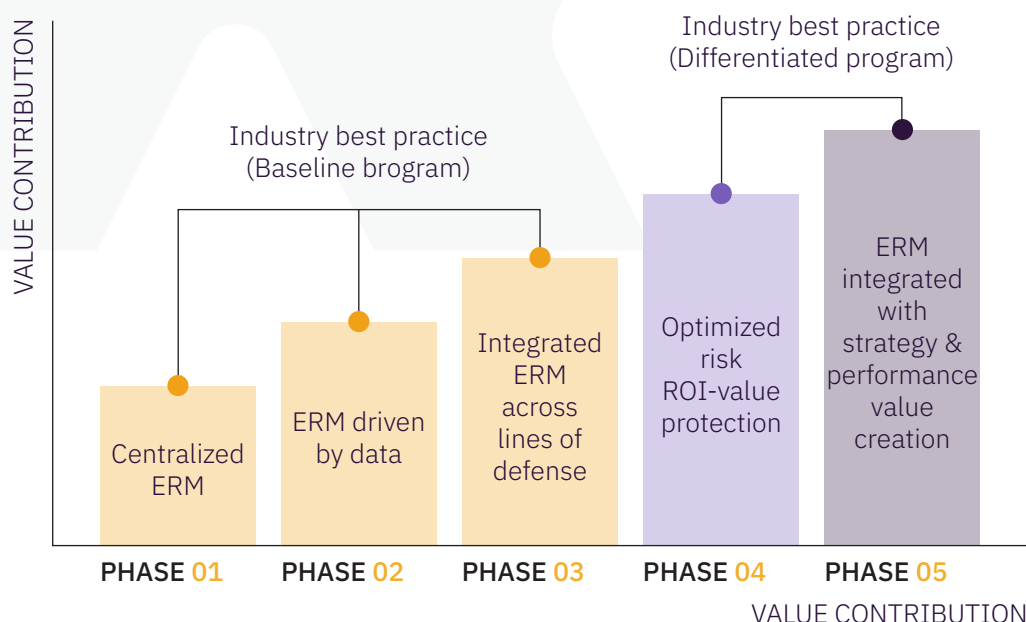
The ERM maturity model

Achieving best practices in risk management takes time and involves progressing through various levels. The important thing is that the three lines of defense are aligned around the ultimate objectives and understand their individual roles.

There is an inevitable learning curve as management in the front lines—as well as those in audit, risk management and compliance roles—transform their processes and discover the best ways to collaborate.

A phased approach is the most effective way to introduce and mature effective risk management. The snapshot below, which is the typical evolution of ERM in most organizations, can be used as a guide.

How mature is your ERM?

VALUE CONTRIBUTION

Industry best practice
(Differentiated program)

Industry best practice
(Baseline brogram)

Centralized ERM

ERM driven by data

Integrated ERM across lines of defense

Optimized risk ROI-value protection

ERM integrated with strategy & performance value creation

PHASE 01　PHASE 02　PHASE 03　PHASE 04　PHASE 05

VALUE CONTRIBUTION

7 considerations for performance-enhancing ERM

ERM is evolving fast, in response to a more dynamic risk landscape and the many opportunities (and threats) from digital transformation. Organizations that embrace purpose-built technology and all of its benefits are winning the race. An intelligent and integrated approach to ERM is the *number one secret to differentiating performance*.

Read on to find out how to achieve an effective ERM program.

01
Move beyond a compartmentalized silo view of risks

An inability to see both the big-picture issues and the minor risks is often the reason why risk management efforts fail.

Managers responsible for operational risks in one business area may not have insights into operational and compliance failures in another area.

Each risk area, when viewed in isolation, may not be a cause for concern in terms of achieving corporate objectives. But a series of apparently low-impact compliance failures can attract the attention of regulatory authorities and the media, quickly resulting in major brand damage or financial penalties. The cause of the problem is often an inability to determine the impact of combining different risk categories.

An advanced risk management process helps you recognize the potential for risk early so you can respond quickly to any early warning indicators that are revealed through trend analysis.

The solution is to implement a framework and oversight system for relating risks to each other. This provides a consistent way of measuring risk impacts on the achievement of corporate objectives by aligning key risk indicators (KRIs) with key performance indicators (KPIs).

02
Provide management with quantified insights into risks

Getting an overview of the current state of organizational risks is a cumbersome and subjective process for many organizations. Risk assessment is often managed with different processes in separate business areas. Consolidating multiple reports and spreadsheets is resource-intensive and frustrating for executives, who end up facing a mix of different risk categories and assessment processes.

ERM technology provides management and the lines of defense with the ability to review up-to-date dashboards reflecting the most current and quantified state of risk assessment, making immediate and informed decision-making possible.

This helps reduce inevitable risk assessment subjectivity and bias, especially in cases where business managers are responsible for completely different business lines, making it difficult to compare and normalize risks.

Fact-based analytics can overcome these weaknesses by normalizing risk assessments, to provide more valid, quantified risk comparison and aggregation.

03
Use big data & analytics for *real-time risk monitoring*

Analyzing multiple data sources gives you the objective ability to put all of your risks in context. Millions of daily operational tasks and financial transactions can be monitored to determine whether, in aggregate, risks are increasing to a point where action must be taken.

Continually monitoring what is actually happening within multiple business processes reveals critical trends and indicators of small issues that could turn into major problems. Analytics also provide insights into new and emerging risks: ones that would otherwise go unnoticed until it's too late.

In 2017, McKinsey reported that 90% of the world's data at that point didn't exist two years earlier—and yet only an incredibly small 1% had actually been analyzed. This means that the potential for data-driven risk assessment and monitoring is enormous, and currently underused.

As organizations mature their risk management processes and capabilities, they typically move from a retrospective and defensive point of view on risk to a more forward-looking one that makes smarter decision-making possible. When this point is reached, risk management practices can enable the organization to perform better. This is because risk professionals can spot obstacles and act quickly to address them.

04
Apply analytics to internal controls

Business operations managers often view internal controls as impediments to "getting the job done." Sometimes these views are justified, especially when controls become expensive to maintain and impact productivity. But a culture in which controls are routinely bypassed or ignored is very risky. So, how do you manage this challenge?

The answer is to rely on analytics to monitor activities continuously. Instances of regulatory non-compliance, fraud, waste and abuse can be monitored and responded to quickly.

The objective is to focus on the bad stuff that is actually happening, not to prevent every possible risky transaction through an unmanageable number of controls. If the risk exposure or financial impact is low, it may be sufficient to simply monitor for instances that violate controls or risk thresholds. And if the impact is high, transactions can immediately be red-flagged.

If employees know a policy is in place and their adherence is being monitored, traditional, cumbersome and often expensive control approaches become less necessary. Data analysis and transaction monitoring allow you to fine-tune a system that's neither overcontrolled nor undercontrolled.

05
Make data-driven risk management decisions

The traditional approach to risk management was risk avoidance, with multiple processes and controls designed to reduce poor decisions, poor performance and compliance failures.

Some executives and business process managers may view ERM as something they do instinctively, as part of their jobs. They take risks and opportunities into account whenever deciding on a strategic course of action. But a word of caution: change is constant—both within and outside the organization—and even the smartest business manager can struggle to stay informed of everything that's actually happening.

High-performance organizations view risk management less as avoiding risks and more about making the most of strategic opportunities. Information is key to this, and dedicated technology to help make sense of the masses of data is essential.

It's never practical to completely eliminate risks. What's important is to understand what's currently happening and the most likely impact on opportunities and strategic objectives, and the impacts of various actions. It's this intelligent and highly informed culture of risk-taking that is now understood to be key to exceptional corporate performance—one that nearly always outperforms a traditional risk-averse culture.

06
Integrate risk management into daily business activities

Opportunity and risk should be viewed as two sides of the same coin. Shifting to this perspective leads to an important outcome: integrating risk management into daily decision-making across the organization.

A smart, risk-intelligent culture means that employees understand how their decisions impact the achievement of corporate objectives. It also means that employees seek to be continually informed about both risks and opportunities—and take a proactive approach to managing both.

A culture that addresses risk and opportunity smartly results in employees who are empowered to take on informed risks, rather than having their performance measured by how much risk they eliminate. As a key part of this organizational culture, scenario analysis and the use of risk dashboards should become a standard part of management practices.

07
Bridge the gap between business & risk professionals

A common challenge to successful ERM is the divide between risk management and business management. Risk professionals don't have the business context to fully understand risks, while business managers lack a practical understanding of the role of risk and compliance control frameworks.

The solution is an integrated approach where risk management frameworks, regulatory requirements, controls and compliance processes are all linked together. This allows both business managers and risk management professionals to see the world through a similar lens and context, and allows them to be confident that they have a single source of truth.

Creating an integrated program—with everybody using one governance, risk and compliance (GRC) technology platform—transforms the traditional disjointed and siloed approach into unified oversight. A unified solution gets the entire organization working together to achieve objectives and drive performance.

Are the following **drawbacks to successful ERM** present in your organization?

Think about the ERM processes in your organization as you read the following common barriers. Do your processes suffer from any of these risky characteristics?

Drawback 1: Spreadsheets

Spreadsheets are incredibly versatile, easy to use and cost-effective, but they're not suited to ERM.

Spreadsheets are difficult to consolidate. Even if the same consistent spreadsheet template is mandated for use across the ERM process, the task of compiling large numbers of spreadsheets is inefficient and frustrating.

Spreadsheets are highly prone to error. Even the best-designed and best-controlled spreadsheet template can get altered unintentionally, resulting in incorrect data. The impacts on assessing enterprise risks can be serious. (And the irony of managing risk with a risky tool undermines credibility in the whole thing!)

Drawback 2: Silos

Multiple silos results in risk management processes that are inefficient and less effective.

You are probably already well aware of the problems with risk management and compliance silos. The extent of the issue varies among organizations, reflecting the way that processes evolve over time.

Various forms of risk management silos often exist for almost every different aspect of risk (including strategic, financial and operational), each of which may have its own subcategories for function, geography or business unit.

From a process point of view (and a technology one), the problem is that every silo takes a different approach to tracking, managing, assessing and reporting risks. The result is inefficient, duplicates efforts and wastes resources.
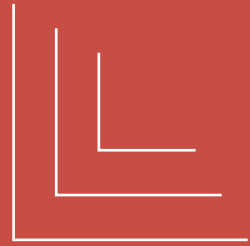
Drawback 3: Complex, customized & costly systems

Risk silos also result in multiple incompatible and duplicate systems and software products.

Another common challenge comes from using technology that was built piecemeal to meet emerging needs (e.g., a spreadsheet system, or a mix of spreadsheets, documents, shareware and multiple network folders). In many cases, a different specialized risk and compliance software tool is acquired for each siloed area.

Many of these technology solutions are inflexible in meeting an organization's growing needs. Forced upgrades from legacy systems or finding newer, integrated solutions often result in increased efforts, license fees and consulting services costs.

What now?
How to get started on the journey to performance-enhancing ERM …

If you have read this far, there's a strong chance that you already know that the ERM processes in your organization need improvement.

What can you do next?

Take a moment to consider how your organization's approach compares to what you have just read:

+ Could your risk and compliance management program deliver more value to your organization if it evolved into a true performance-focused, enterprise-wide process?
+ What benefits could you achieve?
+ What potential obstacles do you foresee?

We have worked with many organizations that were intent on accelerating corporate performance through a better approach to risk management. Purpose-built technology is an essential part of a high-performance ERM process, and RiskBond, Galvanize's risk management solution, has been designed to support the most intelligent and effective processes. It centralizes and simplifies core risk management activities in a single, integrated platform.
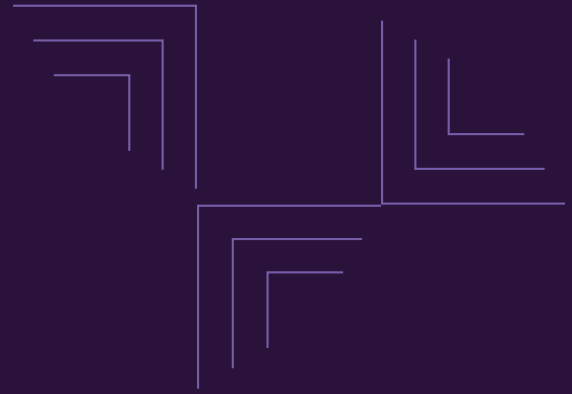
Ready to improve your ERM program & enhance performance throughout your organization?

↳

Galvanize

is now **Diligent**

ABOUT THE AUTHOR
John Verver, CPA CA, CMC, CISA

John Verver is a former vice president of Galvanize. His overall responsibility was for product and services strategy, as well as leadership and growth of professional services.

An expert and a thought leader on the use of enterprise governance technology, particularly data analytics and data automation, John speaks regularly at global conferences and is a frequent contributor of articles in professional and business publications.

ABOUT GALVANIZE

Galvanize, a Diligent brand, is the leading provider of GRC software for security, risk management, compliance and audit professionals. The integrated HighBond platform provides visibility into risk, makes it easy to demonstrate compliance, and helps grow audit, risk and compliance programs without incurring extra costs.

wegalvanize.com