How to achieve excellent Enterprise Risk Management series
www.pwc.com/us/ermexcellenceseries
Article 3: June 2015

How ERM programs evolve

Overview
An organization’s enterprise risk management (ERM) program can be a powerful management tool for achieving strategic and operational objectives, but it can be difficult to maintain and grow over time. After many years of observing different organizations in different industries, we have identified common ERM program development trajectories which can prevent organizations from consistently building and integrating risk management capabilities. Those trajectories include the tendency of ERM programs:

- To start and stop every few years
- To fail to mature beyond the current state
- To build up quickly in response to an event and then atrophy afterward

An ERM program’s success is driven by ongoing identification and implementation of new skills and capabilities. ERM programs should be planned—and flexible, and they should evolve in a strategic manner supported by a common understanding of program objectives and defined steps to improve risk management capabilities. The integration of risk management approaches into strategically important business decisions or processes can provide ongoing evidence and communication of program value and benefits.
This article describes common risk management program trajectories, common pitfalls, and a methodology and long-term plan for supporting a successful and relevant ERM program.

**ERM program expectations**

Organizations are facing increasing pressure from both internal and external stakeholders to align organizational strategies, goals, and risk appetites. The external stakeholders are the board of directors, investors, and regulators. The internal stakeholders are senior management and internal groups affected by ERM program activities. Typically, the driving force behind the development of an ERM program is a question from a board member or senior management, or a data request from a regulator.

Enterprise risk management should be integrated with business decision-making activities at both the executive and operational levels to maximize the return on the organization’s ERM program investment. Information gathered through the enterprise risk management process can create a better understanding of uncertainties—both downside and upside—and recognition of the internal management capabilities required to address them. Such information should be at the heart of business plans, mitigation and monitoring activities, and resource allocation.

Internal and external stakeholders should understand the ERM program’s objectives: how activities help achieve strategic and operational goals and how value is created for the organization. Throughout the ERM program development process, activities should be guided by well-understood business risk management principles specific to that organization. ERM programs should:

- Provide timely and comprehensive risk reports for business decision makers.
- Use existing processes and personnel to monitor and report risks.
- Establish uniform and sustainable risk management processes and a common risk language.
- Keep risk profiles and risk plans up-to-date.
- Encourage open and cross-functional discussions of top risks and major business issues.
- Integrate risk information with planning, compliance, and other business activities.
- Reinforce accountability for risk management by risk owners.

It is important to compare the organization’s actual activities with the foregoing business principles on a regular ongoing basis to ensure development stays aligned with ERM program objectives and integration with business processes.
A primary goal should be to create a sustainable and value-adding ERM program that can survive management turnover, priorities of the month, and resource challenges. That creation can occur only if the risk management program is well defined, has a clear value proposition, and includes a plan to develop, integrate, and institutionalize enterprise risk management capabilities over time across the organization. Effective ERM processes are typically aligned with the corporate calendar, which requires ongoing involvement throughout the year that moves beyond the initial enterprise risk assessment and provides an up-to-date and comprehensive understanding of risks and management capabilities.

Initial questions to answer
- What are the ERM program’s objectives?
- How would you define success—both initially and over the long term?
- Which ERM program elements are working well?
- What are the perceived shortcomings or enhancement opportunities in ERM program design and execution?
- Which enterprise risk management capabilities exist, and which are lacking?

The role of leadership and turnover in ERM program evolution
The importance of leadership support in ERM program development cannot be overstated. Enterprise risk management ownership and guidance have to start at the top to gain initial ERM program buy-in and then to support ongoing investment in people, processes, and systems.

A common challenge is ongoing management turnover, which can derail the process of building ERM program buy-in. New executives may not have the same understanding or want to give the same level of support for enterprise risk management activities as tenured executives do. Some new execs may even consider enterprise risk management a distraction from other business activities.

Having in place a well-understood value proposition helps position enterprise risk management activities as larger than the individuals running the ERM program and as broader than periodic enterprise risk assessment activities. If positioned correctly, the ERM program can be accepted as a management tool that will positively affect the decision-making culture through education, ongoing communication, and targeted risk management information.

Common trajectories for ERM program development
As noted previously, there are several common trajectories for ERM program development. They are described next and are shown in graphic form; time is shown on the horizontal axis and maturity on the vertical axis. Maturity is considered to be the relative level of risk management capabilities related to ERM governance, processes, culture and performance, and infrastructure. Time and discipline are necessary to evolve an ERM program to the desired level of ERM capabilities consistent with long-term ERM program principles and objectives.

ERM program trajectories are:
- **Start and stop.** In this trajectory, management fails to move beyond basic enterprise risk assessment practices. That failure leads to declining interest in the ERM program and uncertainty about the overall value of enterprise risk assessment efforts. Over time, ERM program interest and attention follow the enterprise risk assessment update calendar, which is sometimes extended from quarterly to annually to biannually as interest wanes. Management may describe the enterprise risk management effort as a failure or a one-time project with little value.
• **Start and stagnate.** Interest peaks initially by introduction of new ERM processes such as the enterprise risk assessment and related enterprise risk action plans. The ERM program moves forward using periodic meetings but does not add new capabilities. Because little activity occurs between enterprise risk assessment updates and the enterprise risk assessment, participants mistakenly believe the enterprise risk assessment exercise is itself the ERM program rather than being only a single process component. A consequence of that perception is that management may deem enterprise risk management activities simply a board of directors’ check-the-box exercise requiring only minimal ongoing participation and support.

• **Start slow, react, and atrophy.** An organizational event sometimes triggers recognition of the need for more-mature enterprise risk management capabilities. Triggering events could be going public, integration of an acquisition, or expansion into a different business, a different product, or a new geographic market. These strategic initiatives may involve the development of new or revised strategies, objectives, and related management capabilities; and they’re often followed by declining interest due to lack of sustainable and foundational processes and weak integration of new enterprise risk management capabilities in business decision-making activities.

• **Evolve steadily and consistently.** The least common program trajectory is the consistent introduction and integration of new capabilities to maintain a high level of ERM program interest. A key factor in consistent ERM program development is evolution in a planned but flexible manner, supported by a common understanding of ERM program objectives and defined steps for improving program capabilities. An ERM program value proposition is a critical element in the development and maintenance of support for program improvements and investments.
Drivers and responses for maintaining positive momentum

There are a number of potential challenges to building an effective and sustainable ERM program. However, there are a range of responses that can be effective for each ERM program challenge. Sample challenges and responses are summarized in the following table.

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Response</th>
</tr>
</thead>
</table>
| **Lack of executive support:** Many executives feel overwhelmed by existing responsibilities and do not want more responsibility—particularly for activities that may appear to be of questionable value. In addition, executives sometimes do not see the value produced by the periodic enterprise risk assessment activities and may fail to understand the correlation between a strong and mature ERM program and the achievement of strategic objectives. | • Clearly articulate and communicate the enterprise risk management roles and responsibilities of all key stakeholders—from the board through management and on to functional executives.  
• Understand all roles and responsibilities to prevent finger pointing and confusion, and provide the foundation for ERM process implementation and integration.  
• Educate and train both the board and management on the ERM program’s objectives and activities, as well as alignment with strategic and business goals. |
| **Changing of the guard:** The one certainty in organizations is change. Leadership changes are usually responsible for slowing ERM program implementation, and in the worst cases, can completely stop a program. | • Institutionalize the ERM program so that it is bigger than any one individual involved with the program.  
• Take advantage of the leadership change to review the program and determine which ERM elements are working well and which need improvement. |
| Culture: Many organizations are decentralized and view an ERM program as a form of centralization redundant with the business risk management activities occurring within the individual organizations. Additionally, the decision-making culture may not value deep analysis or the integration of enterprise risk concepts with strategy development. | • Develop and implement a standardized and consistent ERM program, including governance, process, cultural and performance, and infrastructure components.  
• Determine the right level of centralization or decentralization for the ERM program to best integrate with the overall decision-making culture  
• Conduct a series of proof-of-concept pilot exercises to show the value of performing enterprise risk analysis to resolve business issues.  
• Identify desired behaviors and communicate success stories telling how enterprise risk management actions have contributed to the achievement of a business goal. |
| **Poor initial risk program positioning:** ERM programs are sometimes positioned too low in the organization, or they can have poorly understood mandates. | • Elevate the role of enterprise risk management in the organization to that of a senior executive — preferably no more than two levels from the CEO level.  
• Clearly articulate and communicate the goals and objectives of the ERM program at program initiation and periodically as enterprise risk management activities occur.  
• Periodically conduct a comprehensive diagnostic of the ERM program to determine the value the organization is receiving and whether the current enterprise risk management objectives have stayed aligned with the evolving business strategies and environment.  
• Directly clarify any confusion over ERM program activities versus compliance and internal audit activities. |
| **Communication:** We often see a lack of ongoing communication of (1) enterprise risk assessment expectations, (2) current risk management responsibilities and activities, (3) enterprise risk management information, and (4) future ERM program plans. Organizations often fail to consistently articulate the purpose of enterprise risk management or to communicate value—in the form of success stories—and ownership at the level of business activities. | • Have key executives communicate the importance of enterprise risk management through periodic e-mails and presentations.  
• Communicate how ERM program activities integrate with other corporate planned initiatives.  
• Communicate enterprise risk management responsibilities and the expected time commitment. |
| **Lack of risk program discipline:** ERM programs often are developed with the best of intentions, but reality can intervene. After the initial enterprise risk assessment, management might become distracted by other business issues and therefore may be unwilling to invest in developing ERM capabilities. In addition, lack of accountability for not meeting ERM program or risk plan objectives can lead to poor program execution and lack of growth in enterprise risk management capabilities. | • Integrate ERM program responsibilities into the performance management process for all management personnel.  
• Integrate strategic and ERM plan initiatives to alleviate organizational overload, eliminate redundant activities, and close potential gaps in dealing with key risks.  
• Communicate that enterprise risk management is more than a simple enterprise risk assessment and that it involves comprehensive risk identification, judicious prioritization and analysis, careful action planning, close monitoring, and transparent reporting. |
<table>
<thead>
<tr>
<th>Challenge</th>
<th>Response</th>
</tr>
</thead>
</table>
| **Skills gap:** Leading and staffing an ERM program present complex challenges and difficult roles. Enterprise risk management activities require senior executives with strong political skills to navigate organization issues and with strong technical skills to identify, prioritize, and analyze risks. All such skills may not reside in one individual, thereby often requiring teaming to accomplish ERM program objectives. | - Identify desired enterprise risk management capabilities within the ERM program and the businesses.  
- Develop and/or recruit risk leaders with the hard and soft skills needed to support ERM program objectives.  
- Implement enterprise risk management training programs to improve the capabilities of all key stakeholders.  
- Develop and communicate a defined career path for enterprise risk management professionals.  
- Once the ERM program has been established, consider rotating key executives through enterprise risk management leadership positions to spread enterprise risk management capabilities across the organization.  
- Focus on positioning enterprise risk management professionals as trusted business advisors rather than as risk police. |
| **Lack of budget and staffing:** It is a simple truth that a successful ERM program requires committed and dedicated resources. Large organizations cannot be effective executing enterprise risk management responsibilities with only part-time resource commitments. Such lack of resources is often directly tied to the initial ERM program design, lack of a value proposition, and poor ERM program development discipline. Outside support from consultants can bridge an organization, but those consultants’ roles must be clearly defined so that ERM program ownership is clearly understood to reside with the business. | - Prioritize investments in enterprise risk management professionals to be as important as investments in key business executives.  
- Allocate dedicated full-time resources for leadership and staffing to enterprise risk management to improve the likelihood of ERM program success.  
- Use third-party support under management supervision to jump-start the ERM program and to fill management capability gaps. |
| **Lack of a value proposition:** An ERM program needs a value proposition, but enterprise risk management leaders are sometimes unable to articulate value beyond the compliance requirements that drive the program’s implementation. Determining the fundamental drivers of an ERM program is critical to the program’s success: What is the value from enterprise risk management activities? Why invest in people and systems? What is the organization going to gain from the ERM program? Will enterprise risk management activities affect strategic decision making in a positive way? | - Periodically review ERM program objectives, goals, activities, and output.  
- Maintain a development plan with specific actions to be taken for building on what is working and for fixing what is not.  
- Define success, including expected qualitative and quantitative value from the ERM program.  
- Articulate and communicate ERM success stories to the organization to enhance understanding of the value the organization is receiving from its ERM program. |

**The importance of moving beyond the “annual” enterprise risk assessment exercise**

Let’s face it: most of us cannot remember what we were working on at this time last year. Performing ERM program activities—including the enterprise risk assessment—only once a year is simply not enough to maintain strong and up-to-date enterprise risk management information in a manner that supports strategic decision making and positively affects the organization’s culture. Infrequent enterprise risk management activities often require reinventing the wheel, which can undermine ERM program interest and support.

Enterprise risk assessment processes may form the core of an ERM program, but the primary objective should be more than just accomplishing the enterprise risk assessment update. The foundation of an ERM program consists of activities that occur both before and after the enterprise risk assessment: in the forms of the communication, training, analysis, planning, and reporting activities that serve to support the businesses’ actions that in turn respond effectively to enterprise risk issues.
ERM in Action: Company dedicated to integration of enterprise risk management capabilities

Background and ERM program design
A new publicly traded company was created several years ago after being spun off from a larger company. After consulting with its board of directors, the senior management team recognized the need to develop an ERM program that would identify, prioritize, and respond to the company’s biggest enterprise risks. The executives were familiar with the ERM program the previous parent company had in place, and they wanted to make sure their new program would have a higher value and produce information helpful for decision making rather than be a compliance-oriented activity.

The company was in a rapidly changing business environment, competition within the industry was increasing, and the company was faced with price pressures, increased regulation, resource constraints, and complex teaming arrangements with suppliers and competitors. Responsibility for developing the right kind of ERM program was assigned to the treasurer, who received initial guidance to make the program operationally relevant but not redundant with existing enterprise risk management processes at the business level.

Working with a consultant, the treasurer decided the first step should be to determine an enterprise risk management process and governance framework. The ERM program was to be governed by a risk committee assigned to meet quarterly for review of risk management activities, the company’s risk profile, and its risk mitigation activities. Enterprise risk management program objectives and desired risk management capabilities were identified early on to guide all subsequent ERM activities. Meetings were held with a broad group of managers to explain the ERM program development process and to receive their input into program design, including enterprise risk assessment criteria and survey structure. Managers, too, provided valuable input into development of the initial enterprise risk inventory; and the risk inventory was closely aligned with company strategies and strategic initiatives.

Initial enterprise risk assessment
Executive support for the ERM program was integrated into communications before, during, and after the initial risk assessment. Enterprise risk assessment results were summarized and then reviewed with the risk committee. Risk plans were assigned to risk owners for the enterprise risks with the highest risk exposure. The risk plans were then reviewed by the risk committee. An important ERM program element is the quarterly meeting with the board of directors, when risk owners discuss enterprise risk issues and risk plans.

Moving beyond the initial enterprise risk assessment
The company decided early on to prioritize from the enterprise risk assessment process by collecting more information on enterprise risks and risk management capabilities than was initially necessary to prioritize the risks. The information—including detailed risk drivers, risk consequences, and interrelated risks—would form the foundation for building additional risk management capabilities, including risk scenario analysis and risk measurement to better understand select enterprise risks.

- **Deep dives:** For top enterprise risks, the risk exposure and management capabilities were validated through additional data collection and analysis. In some cases, enterprise risks were bigger than expected, which drove changes in risk plans and mitigation strategies (e.g., insurance coverage).

- **Management capabilities:** The enterprise risk assessment process was adjusted in the second year to include a focus on current management capabilities for each risk. Rather than prioritize efforts based solely on risk exposure, the approach was augmented by identifying gaps between management capabilities and risk exposure. That shift helped turn the risk plan discussions into more positive ones by identifying the management capabilities necessary to enable risk taking—including taking additional risks when practical.

- **Risk scenarios:** The base of information collected during the enterprise risk assessment—including risk drivers, consequences, and interrelationships—was applied to construct plausible relevant and challenging scenarios for review by the management team. A scenario analysis process was introduced at the risk committee, and a different scenario is assessed each quarter. The scenarios are constructed with the support of subject matter experts throughout the company. The activity integrated risk language and approaches to real-world business situations, and it supports the desire to integrate enterprise risk management principles into the company’s decision-making culture.

- **Risk profile updates:** The rapidly changing business environment is resulting in ongoing changes to the company’s enterprise risk profile. The enterprise risk profile is discussed at each risk committee meeting, and additions, deletions, and changes are made each quarter. In some cases, the risk committee has overruled the relative-risk rankings from the risk survey based on new information received from risk committee members and subject matter experts.

- **Risk appetite and tolerance:** The risk committee has embraced the concept that risk appetite and tolerance is not a statement but a process whereby the group agrees that the company has more or less appetite for certain businesses, business activities, and risks. It is recognized that risk appetite and risk tolerance change over time and must be monitored and reported. The information gets included as part of the company’s strategic and business plans based on the recognition that risk appetite and tolerance should drive resource allocation.

- **Risk measurement:** Quantification is a means to validate risk exposure estimates. For instance, cybersecurity was identified as a top enterprise risk. The ERM organization worked with the information technology organization, the insurance organization, and subject matter experts to better understand the size of the risk exposure and the company’s current management capabilities. The results included an increased estimate of potential damages from a cyber incident and a restructuring of insurance coverage to offset potential financial losses.

- **Information sharing:** Risk management information is shared with the businesses, support departments, internal audit, and the board of directors.
Developing—and executing—a plan to move forward

It sounds cliché to say that a plan is needed to move an ERM program forward, but a plan should be more than a piece of paper; it should represent a commitment to action. A plan is critical to both ERM program survival and ERM program development. At its most basic, the ERM program development plan should incorporate:

- ERM program objectives
- Metrics for tracking ERM program success
- Resources (internal and external) and processes that will support the ERM program objectives
- Establishment of risk governance structure and enterprise risk management processes that contain risk identification, prioritization, analysis, planning, monitoring, and reporting
- Current and desired enterprise risk management capabilities
- Clearly defined enterprise risk management roles, responsibilities, and authorities
- Desired information to support business decision making
- A communication system for ERM program development and enterprise risk assessment process rollout, covering what has happened, what is happening, what will happen, and value of activities to the organization and the participant
- Current and desired risk culture and desired behaviors
- Consistent ERM program taxonomy, risk inventory, and risk measurement scales
- Opportunities for integrating enterprise risk management approaches and information into business processes and activities
- Time-bound actions with assigned owners
- A value proposition for various company audiences

Listen for potential problem areas

ERM program leaders should remember that people and organizations touched by enterprise risk management activities are not just participants; they are **internal customers seeking a trusted business advisor**. Formal and informal feedback from customers should be used to drive ERM program development.

**Not value adding**—“Why do this? The ERM program acts in a silo at headquarters and just creates pretty charts.”

**Not integrated with underlying business processes**—“I don’t understand or use the information. Do you? For what?”

**Boring**—“If this is just another risk assessment providing little value, then kill me now.”

**Lack of ongoing communication**—“Now that I responded in a timely fashion to the enterprise risk assessment and prepared my risk plan, I have heard nothing nor seen any evidence that this effort has resulted in securing the additional resources and capabilities needed to manage the enterprise risk well. Why the silence? Is my opinion not important?”

**Going through the motions**—“This just seems like a ‘check-the-box’ effort… another quarter, another year, another survey. I see no evidence of tangible actions and results.”

Poor understanding of how to use risk management information: “What do I do with enterprise risk assessment information?”

Poor report design, frequency, and content: “The information is too detailed.” “The information is too high level.” “The information is not focused on my needs, and it is too difficult to generate.” “I do not receive this information in a timely and consistent format.”

Lack of visible senior-executive support: “I don’t know whether my executive or the executive team supports this. They never talk about the ERM program.”

Lack of strategic focus: “The enterprise risk assessment doesn’t even discuss the strategies I focus on. The enterprise risks could be for any company in my industry. Aren’t we already addressing risk initiatives as part of our strategic initiatives? Is this redundant?” “Why are we not aligned with strategic planning?”

Capacity: Why do I have to take on more initiatives when I’m already maxed out?

Not affecting business decision making: “Why go through this if it isn’t positively affecting anything?”

For further information on this topic or the article series, contact:

**Stephen V. Zawoyski**  
Enterprise Risk Management  
Leader  
stephen.v.zawoyski@us.pwc.com

**Michael J. Chagas**  
Enterprise Risk Management  
Director  
michael.j.chagas@us.pwc.com

**Ken Hooper**  
Enterprise Risk Management  
Director  
ken.hooper@us.pwc.com

To view all articles in the How to achieve excellent Enterprise Risk Management series and to subscribe to receive notifications of future publications, visit www.pwc.com/us/ermexcellenceseries.