As the preeminent organization dedicated to educating, engaging and advocating for the global risk community, RIMS, the risk management society™, is a not-for-profit organization representing more than 3,500 corporate, industrial, service, nonprofit, charitable and government entities throughout the world. RIMS has a membership of approximately 11,000 risk practitioners who are located in more than 60 countries. For more information about the Society’s world-leading risk management content, networking, professional development and certification opportunities, visit www.RIMS.org.
We are nearly a decade removed from the financial crisis, a cataclysmic event that proved to be a substantial boost for the adoption of enterprise risk management. In 2017, financial institutions led the pack in adoption and advanced ERM practice, a situation no doubt spurred along by regulation and intense scrutiny of the industry since that harrowing autumn in 2008. Nearly half of financial industry respondents this year reported that regulatory requirements were the impetus behind their organization’s enterprise risk management program.

Enterprise risk management’s march toward ubiquity is not contained to the financial sector, however. In the 2013 ERM Survey, we reported that adoption of enterprise risk management practices had reached a tipping point with more than half stating that they had fully or partially integrated programs. Based on the results of our 2017 survey, enterprise risk management continues to show its value with nearly three-quarters of the organizations reporting fully or partially integrated programs. Interestingly, a portion of those who said they did not have an ERM program indicated that their organizations do have a strategic risk management, a governance risk and compliance (GRC) or similar program in place (see figure 1).

On top of the slow-but-sure increase in the practice of enterprise risk management, we see evidence that the quality of ERM is improving as well. Respondents in 2017 reported that their organizations’ effectiveness at key ERM activities are at improved levels compared to 2013. The financial crisis might fade farther into the rearview mirror, but that is not diminishing the enthusiasm for enterprise risk management. This is good news for ERM experts and risk professionals in general: This risk management process-cum-general management discipline has staying power.

There is still work to do. Enterprise risk management is a proven way to boost risk management practices and even overall firm value.¹ Yet, only a quarter of organizations are using this powerful discipline in a fully integrated way. Nearly half of respondents (49%) say their organizations have not developed any risk appetite or risk tolerance statements at any business level. And 61% say that their ERM program is being used to inform and influence corporate strategy. A strong tally, yes, but given the value that ERM can easily impart to strategy formation and operating performance, that percentage should be higher (see figure 2).

Respondents in 2017 pointed to a need for improvement for a number of elements of their organizations’ risk practices. Creation of enterprise value through ERM, adoption rate of ERM practices throughout the organization and alignment of risk management with strategic decision-making are just a few areas where respondents feel more dissatisfied than satisfied. A majority of respondents said that their organizations need to mature to a higher level of every attribute of the RIMS Risk Maturity Model™.²

All of that said, we should not lose sight of the fact that ERM has made steady gains in all industries. The fact that more than half of the respondents reported their ERM programs are informing and influencing strategy is a testament to this discipline’s value. RIMS hopes you find the full results of this report to be informative for your own efforts.

---

2 For more on the RIMS Risk Maturity Model™, please visit: https://www.rims.org/resources/ERM/Pages/RiskMaturityModel.aspx
MORE HIGHLIGHTS

62%...say the risk management department is primarily responsible for ERM. In 2013 it was 56%.

48%...say their ERM reports/outputs are reviewed at the board level by the audit committee.

70%...of financial institutions have a board-level risk committee that reviews outputs.

25%...are using ISO 31000 as their guide.

29%...are using COSO (37% of financial companies).

20%...say their program does not follow a particular standard or framework.
...said the primary value of ERM in 2013 was increasing risk awareness.

...say avoiding and/or mitigating risk is a primary benefit.

...say that increasing risk awareness is the primary value of ERM in 2017.

...say eliminating internal silos is a primary benefit.

Top three things executive management expects ERM to deliver:

» Reasonable assurance that major risks are identified.
» Minimized operational surprises and reduced losses.
» Aligned risk appetite and strategic risk management.

We asked those who do not have an enterprise risk management program why that is so. Here are some of the things that they said:

The challenge we are facing is ownership of the enterprise risk management assessment. For us to achieve the expected value of ERM, business units need to be more involved in the process.

ERM is just a shell in our department. Hesitancy to use ERM is primarily due to NOT really wanting transparency. Silo mentality is still going strong.

It’s a never-ending challenge. We are required to perform extensive risk management, but chronically lack funding, staff and CEO support to realize the potential of the function.

Really tough to get executive level buy-in to implement ERM. Currently no interest in our organization (mostly due to limited cost and staffing resources).
RESULTS

Question 1.
To what extent has your organization adopted or is considering an enterprise risk management (ERM) program?

- Have fully integrated ERM program to address risk across the organization (practiced at corporate level and within every business unit): 24% (▲4% from 2013)
- Have partially integrated ERM program (practiced at corporate level or at one or more business unit): 48% (▲6% from 2013)
- Have begun to investigate an ERM program, but have not advanced further toward implementation: 13%
- Do not have an ERM program, but are planning to implement one in the next year: 2%
- Do not have an ERM program and have no plans to look into it within the coming year: 12% (▼6% from 2013)

Results reveal that the trend from ERM’s “early majority” adoption status in 2009 to a more widely accepted management discipline continues. In these latest numbers, 73% of respondents have a fully integrated or partially integrated ERM program in place, compared to 63% in 2013. In the financial industry, ERM is de rigueur: 92% of companies have a fully integrated or partially integrated program.

Financials

- 34%
- 58%
- 3%
- 0%
- 5%
Question 2.
How would you rate the effectiveness of your organization in the following ERM activities? (5 = highly effective; 1 = not effective at all)

- Taking action on identified important and relevant risks: 3.8 (▲1.6 from 2013)
- Anticipating and managing emerging risks: 3.3 (▲0.7 from 2013)
- Instilling awareness of risk as a decision-making discipline: 3.3 (▲0.8 from 2013)
- Linking risk management with corporate strategy and planning: 3.2 (▲0.5 from 2013)
- Clearly articulating risk appetite and tolerances: 3.1 (▲0.2 from 2013)

Effectiveness is up across the board. The biggest change in effectiveness is in “Taking action on identified important and relevant risks.” This is one of the 2017 survey’s most encouraging findings—ERM is moving beyond heat maps and risk registers and into the realm of an organization’s decision-making process. To that point, the second-biggest positive change is “Instilling awareness of risk as a decision-making discipline throughout the organization.”

Question 3.
Are insights from your organization’s ERM program being used to inform and influence corporate strategy?

- 60% Yes
- 27% Not sure
- 13% No

This year was the first time this question has been asked as part of the ERM Benchmark Study, and we can see that more than half of ERM programs are influencing corporate strategy. The evolution of ERM from comprehensive risk identification and mitigation program to an important shaper of strategy is evident by this response.
Question 4.

What motivated the implementation and/or expansion of the enterprise risk management program at your organization?

- Board directive: 28% (Financial organizations: 12%)
- Regulatory requirements: 18% (Financial organizations: 48%)
- Risk manager: 16%
- Audit: 6%
- Grass roots success: 3%
- Rating agency requirements: 3%
- Financial crisis of 2008: 2%
- Investors/owners: 1%
- Banks/creditors: 0%
- Other: 12%
- Don’t know: 10%

Open-ended responses for “Other”:

- Desire to be a premier company.
- Potential financial benefits.
- Single large operational loss.
- A consultant study and the president of the board/CEO.
- ERM happened slowly from the bottom up.
- Working to become public company/SEC requirements.
Question 5.
The primary value we gain from our ERM program is:

- Avoiding and/or mitigating risk: 24%
- Increasing risk awareness: 24% (▼9% from 2013)
- Eliminating silos, e.g., viewing the entire portfolio of risks: 20% (▲7% from 2013)
- Increasing certainty in meeting strategic and operational: 16%
- Compliance with regulatory and legal requirements: 10%
- Providing assurance to shareholders: 3%
- Uncovering untapped opportunities: 1%
- Consolidating processes, e.g., efficiency in data collection: 1%
- Other: 1%

One in five respondents (and more than one-quarter of financial institutions) say that eliminating silos is the primary value. Increased risk awareness was cited as the primary value by 24%, down from 33% in 2013. Even so, increased risk awareness remains an important value, with 42% reporting it as a secondary value.

Question 6.
Please identify secondary value that you gain from your ERM program (select up to three).

- Increasing risk awareness: 42%
- Avoiding and/or mitigating risk: 33%
- Eliminating silos, e.g., viewing the entire portfolio of risks: 29%
- Increasing certainty in meeting strategic and operational: 28%
- Compliance with regulatory and legal requirements: 24%
- Consolidating processes, e.g., efficiency in data collection: 13%
- Providing assurance to shareholders: 13%
- Uncovering untapped opportunities: 8%
- Other: 1%

And yet...
Question 7.

Executive management expects the ERM program to deliver (select your top three):

- Reasonable assurance that major risks are identified, prioritized, managed and monitored (87%)
- Minimized operational surprises and reduced losses (54%)
- Aligned risk appetite and strategic risk management frameworks (integrate risk appetite within strategy setting and execution processes) (44%)
- Improved certainty in delivering organization’s business plans (31%)
- Integrated assessments/responses for interdependent risks (22%)
- Risk analyses for more efficient capital allocation/use in making capital decisions (20%)
- Risk practices designed to improve the success of investments/acquisitions/projects (15%)
- Verifiable financial savings/cost avoidance (12%)
- Favorable evaluations by investors, rating agencies, bankers or other stakeholders (11%)
- Other (3%)

A strong majority of respondents (87%) report that their executive management views enterprise risk management as an identification and monitoring exercise. ERM professionals, by their own admission, have some work to do to convince executives of the additional value discussed in the previous two questions.
**Question 8.**

Are you satisfied or dissatisfied with the following elements of your organization’s risk management practices over the past year?

<table>
<thead>
<tr>
<th>Area</th>
<th>Satisfied</th>
<th>Dissatisfied</th>
<th>Neither</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting to the board on risk issues</td>
<td>189</td>
<td>54</td>
<td>64</td>
</tr>
<tr>
<td>Understanding of risk issues among business units</td>
<td>181</td>
<td>78</td>
<td>48</td>
</tr>
<tr>
<td>Internal communications on risk issues among risk functions</td>
<td>127</td>
<td>103</td>
<td>77</td>
</tr>
<tr>
<td>Risk intelligence capabilities for uncovering risks</td>
<td>96</td>
<td>121</td>
<td>90</td>
</tr>
<tr>
<td>Adoption rate of ERM practices throughout the organization</td>
<td>94</td>
<td>127</td>
<td>86</td>
</tr>
<tr>
<td>Alignment of risk management with strategic decision-making</td>
<td>92</td>
<td>140</td>
<td>75</td>
</tr>
<tr>
<td>Creating enterprise value through ERM practices</td>
<td>85</td>
<td>122</td>
<td>100</td>
</tr>
<tr>
<td>Organizational performance management tied to management’s effectiveness in handling risk issues</td>
<td>83</td>
<td>122</td>
<td>102</td>
</tr>
</tbody>
</table>

Enterprise risk management professionals are optimistic about their programs’ ability to increase understanding of risk throughout the organization. On the internal communications front, ERM is doing well. Risk professionals are still mostly dissatisfied with the state (or lack thereof) of performance management being tied to handling risk issues, and with articulating ERM practices into enterprise value.

**Question 9.**

With respect to ERM in your organization, the department that is primarily responsible for directing ERM activities is:

- Risk management: 62%
- Finance: 11%
- Internal audit: 9%
- Strategy: 5%
- Legal: 5%
- Compliance: 4%
- Other: 6%

In 2017, 62% report that it is the risk management department that is primarily responsible for enterprise risk management. Fewer than in 2013 say it is finance or internal audit departments. These results point to the continued evolution of what risk management departments focus on. Increasingly, it is less about insurance portfolio management and more about enterprise-wide thinking, value creation and protection.
Question 10.  
At the board level, who is reviewing ERM reports and outputs? (Select all that apply):

- Audit committee: 48% (▼3% from 2013)
- Risk committee: 43% (▲4% from 2013)
- Full board of directors: 40%
- Finance committee: 14%
- Governance committee: 14%
- Executive/Compensation committee: 8%
- No regular reviews in place: 4%
- Other: 4%
- Don’t know: 5%

Board risk committees are gaining traction. In 2013, the full board was reviewing the outputs in 49% of cases, compared to 40% in 2017. Risk committee review is increasingly common, as is executive committee review.

Question 11.  
How often does the top risk executive report to the board or board committees charged with enterprise risk oversight?

- Quarterly: 42% (Financial organizations: 68%)
- Annually: 22%
- Semi-annually: 17%
- As needed: 9%
- Monthly: 2%
- Other: 4%
- Doesn’t report: 3%

...
Question 12.
Which risk functions within your organization are included in ERM activity planning and execution?

<table>
<thead>
<tr>
<th>Function</th>
<th>2017 Percentage</th>
<th>% Change from 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT risk management</td>
<td>78%</td>
<td>▲14%</td>
</tr>
<tr>
<td>Compliance</td>
<td>71%</td>
<td></td>
</tr>
<tr>
<td>Business continuity</td>
<td>70%</td>
<td>▲11%</td>
</tr>
<tr>
<td>Operations/safety</td>
<td>68%</td>
<td></td>
</tr>
<tr>
<td>Strategic planning</td>
<td>65%</td>
<td>▲4%</td>
</tr>
<tr>
<td>Legal</td>
<td>64%</td>
<td></td>
</tr>
<tr>
<td>Internal audit</td>
<td>63%</td>
<td></td>
</tr>
<tr>
<td>Human resources</td>
<td>53%</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>49%</td>
<td></td>
</tr>
<tr>
<td>Public affairs/relations</td>
<td>36%</td>
<td></td>
</tr>
<tr>
<td>Logistics</td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>9%</td>
<td></td>
</tr>
</tbody>
</table>

IT risk management has a noticeable shift toward greater enterprise risk management involvement, with 77% of respondents including that function compared to 63% in 2013. Not surprisingly, this increased involvement signals the increasing attention being paid to cyber-related issues. Another function that has become more involved in ERM activity and planning is business continuity, with 60% involved in 2013 compared to 70% in 2017. Involvement of the strategic planning function grew to nearly 65% from 61% in the responding organizations. Other key functions include operations/safety, compliance, internal audit and legal.
COSO and ISO continue as the two main sources for risk management guidance according to our 2017 survey. COSO is the standard used in 29% of cases and ISO 31000 is used by a quarter of respondents. Awareness and use of guidance documents appears to have increased. In 2013, 26% of respondents said that their programs were unaligned; this year that is only 20%.
Question 14.

Have you developed risk appetite and/or risk tolerance statements within your organization? Check all that apply.

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, enterprise level</td>
<td>37%</td>
</tr>
<tr>
<td>Yes, business unit or divisional level</td>
<td>15%</td>
</tr>
<tr>
<td>Yes, departmental level</td>
<td>8%</td>
</tr>
<tr>
<td>No, have not developed risk appetite/tolerance statements</td>
<td>49%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
</tbody>
</table>

As in the 2013 results, nearly half of respondents say that they have not developed risk appetite and/or risk tolerance statements at their organizations. Financial organizations, on the other hand, are generally required by regulators to develop enterprise-wide risk tolerance and/or risk tolerance statements. While 78% of respondents from that industry report that they have developed risk appetite and/or risk tolerance statements at the entity level and 42% at the business level, one would expect a higher rate, given regulatory requirements.

For more on developing risk appetite and risk tolerance statements, see the RIMS Executive Reports, “Steps to Successful Risk Taking: Developing Effective Risk Appetite and Tolerance Statements” and “Exploring Risk Appetite and Risk Tolerance.”

Open-ended responses for "Other":

- Yes, but interpretation of the statements is confusing.
- I have developed and proposed risk appetite/tolerance statements but can't get traction from executives.
- [They are] based on CEO's appetite and tolerance.
Question 15.
Which outside resources have you used (or are planning to use) to develop/implement your ERM program? Check all that apply.

- RIMS: 51%
- Risk management consultant: 37%
- Broker: 30%
- Other associations: 27%
- Financial/management consultant: 21%
- Universities: 19%
- Accounting firm: 19%
- None: 9%
- Don’t know: 8%

Question 16.
If you do not have an ERM program, do you have a similar program like one of the following?

- 12% Strategic risk management (SRM)
- 40% Other
- 48% Governance risk and compliance (GRC)
**Question 17.**
Based on the following RIMS Risk Maturity Model™ attributes, I believe my ERM program is at the following maturity level:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Ad-hoc or nonexistant</th>
<th>Initial</th>
<th>Repeatable</th>
<th>Managed</th>
<th>Leadership</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERM process management</td>
<td>13</td>
<td>20</td>
<td>20</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Adoption of ERM-based approach</td>
<td>11</td>
<td>23</td>
<td>24</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Uncovering risks (and opportunities)</td>
<td>2</td>
<td>14</td>
<td>20</td>
<td>21</td>
<td>6</td>
</tr>
<tr>
<td>Business resiliency and sustainability</td>
<td>3</td>
<td>14</td>
<td>20</td>
<td>22</td>
<td>4</td>
</tr>
<tr>
<td>Risk appetite management</td>
<td>10</td>
<td>12</td>
<td>16</td>
<td>18</td>
<td>7</td>
</tr>
<tr>
<td>Performance management</td>
<td>6</td>
<td>17</td>
<td>20</td>
<td>15</td>
<td>5</td>
</tr>
<tr>
<td>Root cause discipline</td>
<td>8</td>
<td>15</td>
<td>25</td>
<td>11</td>
<td>4</td>
</tr>
</tbody>
</table>

**Question 18.**
Based on the following RIMS Risk Maturity Model™ attributes, which do you want to mature to a higher level?

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncovering risks (and opportunities)</td>
<td>51</td>
<td>12</td>
</tr>
<tr>
<td>Root cause discipline</td>
<td>50</td>
<td>13</td>
</tr>
<tr>
<td>Performance management</td>
<td>49</td>
<td>14</td>
</tr>
<tr>
<td>Business resiliency and sustainability</td>
<td>48</td>
<td>15</td>
</tr>
<tr>
<td>ERM process management</td>
<td>46</td>
<td>17</td>
</tr>
<tr>
<td>Risk appetite management</td>
<td>45</td>
<td>18</td>
</tr>
<tr>
<td>Adoption of ERM-based approach</td>
<td>39</td>
<td>24</td>
</tr>
</tbody>
</table>
As we saw earlier, when asked why an organization does not yet practice enterprise risk management, risk managers identify some age-old hurdles: unclear ownership of the program, silo mentality, lack of funding and lack of executive interest are specifically called out.

These bureaucratic issues are familiar to almost every organization. Yet, despite that, the practice of enterprise risk management continues to spread. For a business practice to be able to weather scrutiny and time, it must provide important advantages. As many organizations that have embraced ERM will attest, this risk management approach provides just that. RIMS believes that enterprise risk management’s expansive view of an organization and its risks, as well as the value that it can add to strategy and executive decision-making, suggests that more organizations will adopt the practice in the coming years.

**CONCLUSION & DEMOGRAPHICS**

**Question 1.**
Please identify your organization’s industry

- 13% Manufacturing
- 6% Health care
- 5% Retail
- 15% Financial Services
- 5% Professional Services
- 6% Energy
- 6% Utilities
- 7% Education
- 1% Telecommunications
- 3% Information Technology
- 12% Government or Non-Profit
- 3% Hospitality
- 1% Industrial
- 1% Telecommunications
- 13% Other
- 5% Retail

**Question 2.**
What is your organization’s estimated annual revenue (US$)?

- 50% More than $1 billion
- 18% $100 million–$500 million
- 16% $500 million–$1 billion
- 3% $50 million–$100 million
- 6% $10 million–$50 million
- 4% $1 million–$10 million
- 3% Up to $1 million
Question 3.
How many total employees are in your organization?

- 17% More than 25,000
- 13% 5,000–10,000
- 9% 10,000–15,000
- 6% 15,000–25,000
- 5% 0–100
- 4% 250–500
- 31% 1,000–5,000
- 10% 500–1,000
- 10% 500–1,000

Question 4.
What is your primary country of residence?

- 79% United States
- 12% Canada
- 2% New Zealand
- 5% Other
- 1% Brazil
- 1% Australia