Federal Enterprise Risk Management

2018 Survey Results

The 2018 Federal ERM Survey is Guidehouse's fourth annual survey performed in collaboration with the Association for Federal Enterprise Risk Management (AFERM). It is designed to provide Federal risk managers and leadership with perspective on the current state and trends of ERM in the U.S. Federal government.

AFERM
Association for Federal Enterprise Risk Management

Guidehouse

Table of Contents

Executive Summary

For the fourth consecutive year, the Association for Federal Enterprise Risk Management (AFERM) and Guidehouse have collaborated to survey Federal government leaders and staff for their insights into the current state of Enterprise Risk Management (ERM) in their organizations.

The overall results for this year's survey are reminiscent of previous years, **demonstrating limited capability maturity in many areas of Federal ERM. Many of the same structural and cultural barriers continue, limiting the generation of organizational benefits**.

One exception to this trend continues to be seen in the improved outcomes for organizations which have **had an ERM program in place for three or more years. A core conclusion is that ERM is a journey and persistence helps drive capability maturity that leads to enhanced results**.

A new theme emerged this year as well, providing evidence regarding the positive impact that Chief Risk Officers (CROs) are having on their organizations. **More pronounced than ever before, organizations with ERM programs run by a CRO exceed the performance levels of those programs that do not have a formal CRO**. This result is evident in the degree to which ERM programs are integrated with other management processes, in embracing the cultural aspects of ERM, and in overall program effectiveness and benefits of ERM programs. We added a section to this year's survey report (*CRO Impact on Federal ERM Programs*) to provide detailed insight into the nature and magnitude of this positive trend for organizations that have entrusted their ERM program in the hands of a CRO.

Top 10 Additional Findings

The following is a summary of the additional significant insights from this year's survey, in no particular order:

- Enhanced management decision-making is broadly realized as a benefit from Federal ERM programs, but none of the other benefits in the survey are being realized by more than a quarter of respondents.
- Cyber Security/Privacy Risk is identified as the top risk area (both current and anticipated in the near future), followed by Human Capital Risk and Operational/Programmatic Risk. In contrast, a number of risk areas were identified as receiving significant management focus and resources despite low perception of actual current and anticipated risk.
- Training & Awareness is highlighted as the top area of focus over the next 12 months. This is consistent with the results that less than a third of organizations are currently providing sufficient risk management training.
- With its highest result in the history of the survey, OMB Circular A-123 represents the primary motivator for the establishment of a Federal organization's ERM program, particularly for larger organizations and those with newer ERM programs.
- Integration of ERM programs with other management processes such as strategic planning, performance and execution processes, and budgetary processes remains low, with the latter representing the least integration.
- The results from the culture-related ERM questions all score, on average, at the midpoint response level or below. There was, however, a notable increase in providing a risk transparent environment that promotes open risk discussions between managers and staff.
- The results from the performance evaluation section on ERM capabilities also score below to the midpoint response level on each question, with the best result related to how well organizations view the effective management of risk as a value add/organizational advantage.
- The top three barriers to establishing a formal ERM program remain unchanged from a year ago: (1) Bridging silos across the organization, (2) Executive-level buy-in and support, and (3) Rigid culture and resistance to change.
- The top three impactful improvements organizations can make to better position themselves for effective risk management are: (1) Tone-at-the-top, Executive support for risk management, (2) Culture change to accept risk management as part of day-to-day business, and (3) More clear linkage, alignment, or integration of risk with strategy and performance.
- Fewer than 10% of organizations across any of our demographic groups indicate having a well-understood risk appetite statement that is integrated into strategy and decision-making.

Organization of the Report

This year's report groups the survey results into four broad categories:

- Characteristics of Federal ERM Programs
- Focus & Priorities
- Execution & Performance
- CRO Impact on Federal ERM Programs *(new for 2018)*

Subsections are included for each category. In context of these categories, the results from this year's survey responses are provided, along with comparison results from the 2017 survey. Analysis is also included based on the primary insights from the data at the aggregate level as well as across a number of demographic breakdowns.

David Fisher
Managing Director
Guidehouse
Risk Consulting Leader

Peggy Sherry
President
Association for Federal Enterprise Risk Management (AFERM)

Survey Approach & Demographics

This report provides the results of the fourth annual survey conducted by Guidehouse (formerly PwC Public Sector) and AFERM on Enterprise Risk Management in the U.S. Federal government. The vast majority of questions are repeated from last year's survey to enable the tracking of trends over time.

The report's bar charts include data from the 2017 and 2018 surveys, except in the case of the small number of new questions, or new answer choices for previous questions, for which only this year's results are provided. To simplify the presentation of the data in these bar charts, percentages have been rounded to the nearest full percent. As a result, the sum of the percentages that are displayed may not equal exactly 100%.

The survey was administered between July 20 and August 13, 2018. Links to the online survey were sent to government members of AFERM, as well as to select leaders in the Federal ERM community who were not AFERM members at the time of the survey. The survey was only distributed to government personnel. While all respondents received the same set of initial questions, subsequent questions followed one of two prescribed paths based on whether the respondent's organization had already implemented an ERM program.

Given that a random sample was not used to select the survey population, this approach represents a nonprobability sample which may not be generalizable to the entire Federal population. However, the survey respondents did span the breadth of the Federal government and across a number of demographic categories. In terms of organizational representation, responses were received from a total of 21 Federal organizations (all but one from the Executive Branch), including 12 of the 15 Cabinet agencies. In many of these cases, additional variety was represented across multiple components or bureaus of these broad departments or agencies.

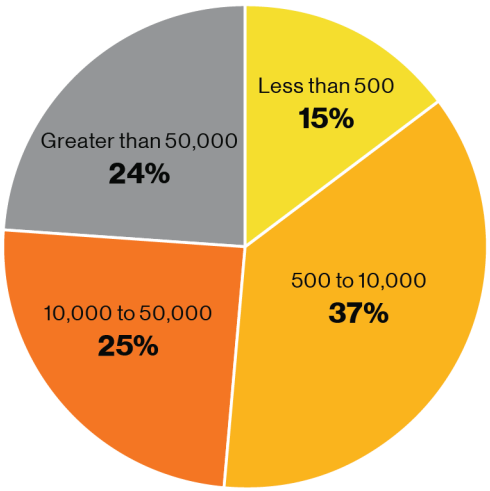
The 21 organizations from which responses were received include the following (in alphabetical order):

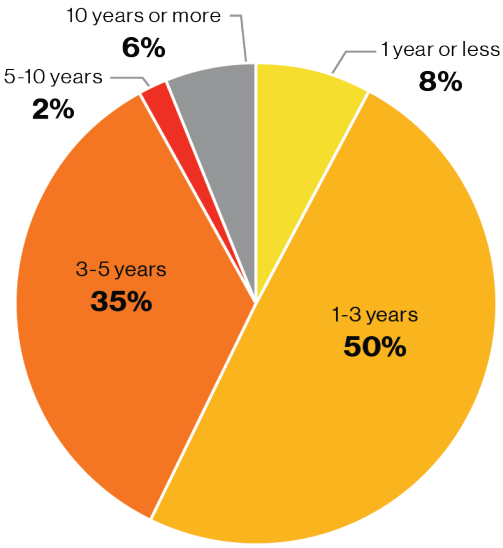
- Architect of the Capitol
- Corporation for National and Community Service
- Department of Commerce
- Department of Defense
- Department of Education
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
- Department of Housing and Urban Development
- Department of Justice
- Department of State
- Department of the Treasury
- Department of Transportation
- Department of Veterans Affairs
- Federal Deposit Insurance Corporation
- Federal Retirement Thrift Investment Board
- National Aeronautics and Space Administration
- National Archives and Records Administration
- National Credit Union Administration
- National Science Foundation
- Securities and Exchange Commission

While personally identifiable information was not requested from survey respondents, some demographic information about their role and organization was captured. The demographic categories were selected with an expectation that the survey results might vary in a material way across these sub-categories and thereby provide additional depth to the analysis and insights. Specifically, the following demographic information was obtained:

Size of your Organization, by number of employees.

To simplify the analysis associated with the size of organizations, the two smallest response categories are combined in the narrative portion of this document and referred to as "**smaller organizations**" (~52% of respondents, less than 10,000 employees) while the two largest response categories are combined and referred to as "**larger organizations**" (~49% of respondents, more than 10,000 employees).





How long has your Organization practiced ERM?

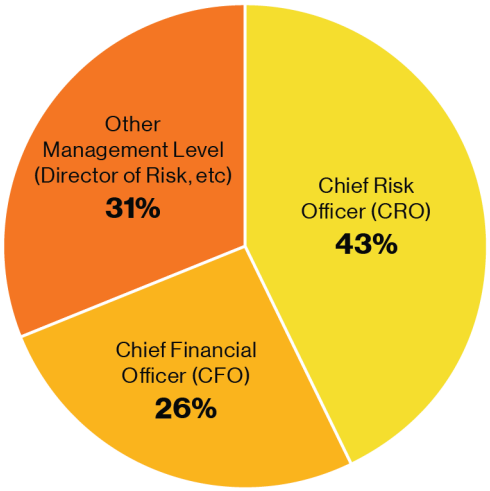
To simplify the analysis associated with the duration of ERM practice within organizations, the two shortest duration response categories are combined in the narrative portion of this document and referred to as organizations with "**shorter duration ERM programs**" (58% of respondents, less than three years of an ERM program) while the category with the longest duration is referred to as organizations with "**longer duration ERM programs**" (42% of respondents, more than three years of an ERM program).

Note: Responses to this question are only from people who work for an organization that already has an ERM program.

Which of the following titles best describes the person responsible for your Organization's Enterprise Risk Management program?

To analyze the effectiveness of Chief Risk Officers (CRO) and the value that they bring organizations, the narrative portion of this document refers to "**CRO-led ERM programs**" (43% of respondents) while the responses that indicate any other leadership are combined and referred to as "**non CRO-led ERM programs**" (57% of respondents).

Note: Responses to "other management" include COO, Deputy Secretary, Comptroller, and others. In addition, responses to this question are only from people who work for an organization that already has an ERM program.



In each section of this report, the analysis focuses primarily on current year results along with relevant comparisons to the previous year's survey. Additional analysis associated with the demographic categories highlighted above is also provided. In particular, instances are highlighted where specific demographic breakdowns demonstrated deviations from the overall results or where clear distinctions between the demographic categories are found.

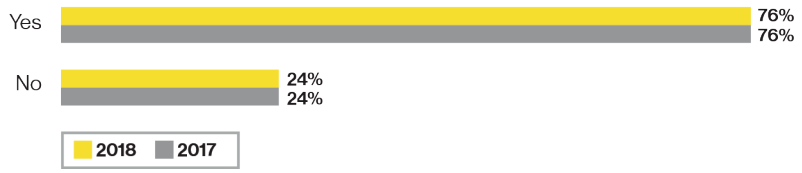
Survey Results

ERM Existence, Duration, and Budgets

In a number of areas, the FY18 survey identifies little difference from the FY17 results. For example, **roughly three-quarters of this year's respondents indicate working in an agency that has a formal ERM program**, virtually unchanged from a year ago.

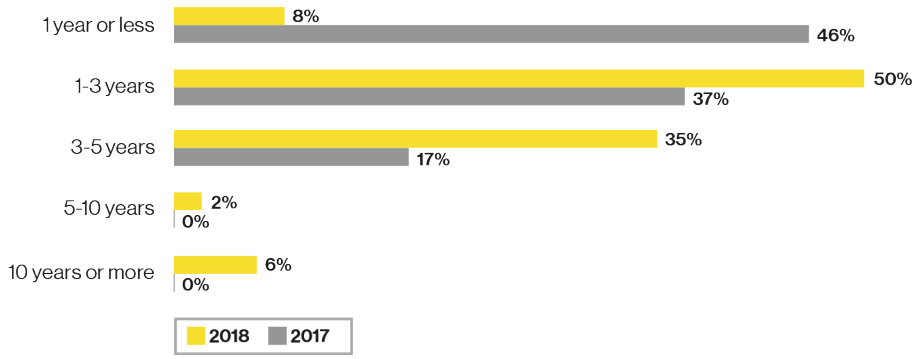
Characteristics of Federal ERM Programs

Q: Does your Organization have a formal Enterprise Risk Management program?



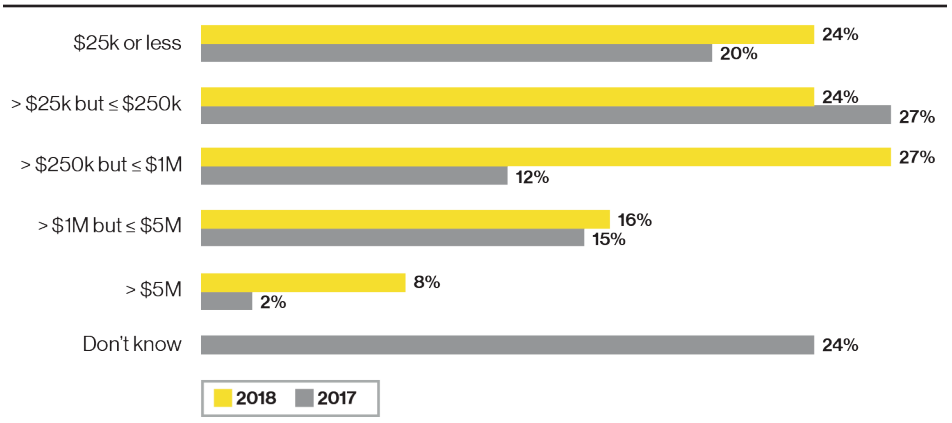
After a surge in new ERM programs starting up last year, very few new programs emerged in FY18, with **only 8% of respondents indicating the initiation of a new ERM program at their organizations in the last 12 months**. Reflecting the large influx of new ERM programs the previous year, **a majority of respondents indicate their organization has a program that is less than three years in duration (58%)**. Organizations whose ERM programs are led by a Chief Risk Officer (CRO) tend to be longer duration programs, with 60% of these programs in existence for more than three years.

Q: How long has your Organization practiced Enterprise Risk Management?



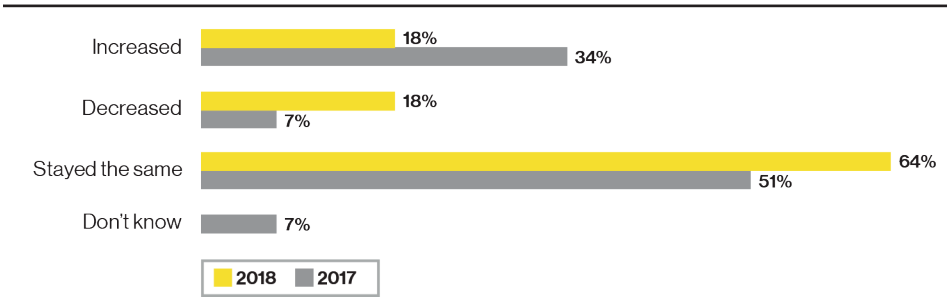
Budgets for ERM programs remain relatively small, consistent with the past three surveys. **Three-quarters of this year's respondents indicate an annual ERM budget of *less* than $1 million**, slightly higher than last year. Larger organizations are more likely to have an ERM program budget *greater* than $1 million when compared to smaller organizations (40% to 14%). **For the shorter duration ERM programs, 91% have budgets *less* than $1 million**, compared to 56% for the longer duration programs.

Q: What is the total annual budget for Enterprise Risk Management activities across your Organization?



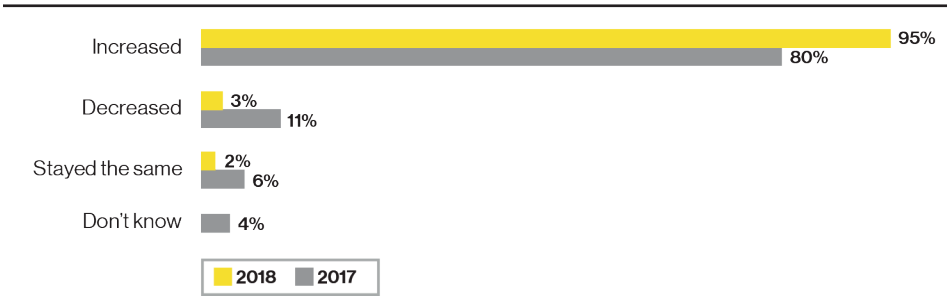
Budgets for ERM programs remained relatively flat over the past year for well over half the respondents (64%), which is consistent across all demographic groups.

Q: In the last 12 months, the budget for overall Enterprise Risk Management activities has done which of the following at your Organization?



Flat budgets over the past year are not correlated to the expected increase in demand for evidence of effective ERM activities over the next three years. There is a **nearly universal expectation (95%) that the demand for effective ERM activities is going to increase**, up from 80% the previous year. That 95% figure is consistent across all demographic groups.

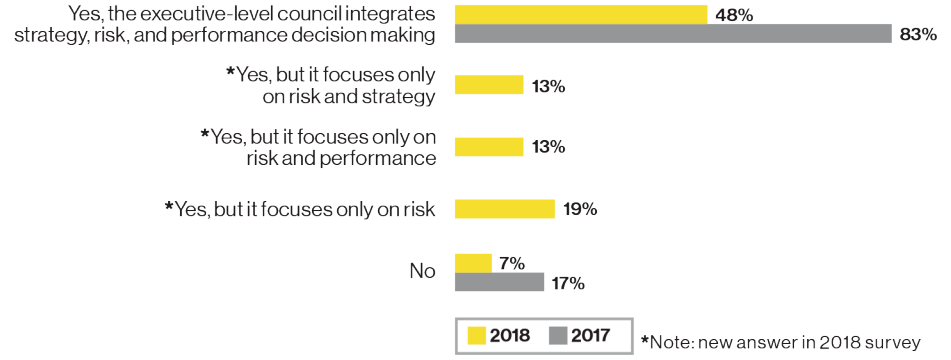
Q: Do you believe the demand for evidence of effective Enterprise Risk Management activities will increase or decrease over the next three years?



Governance & Program Scope

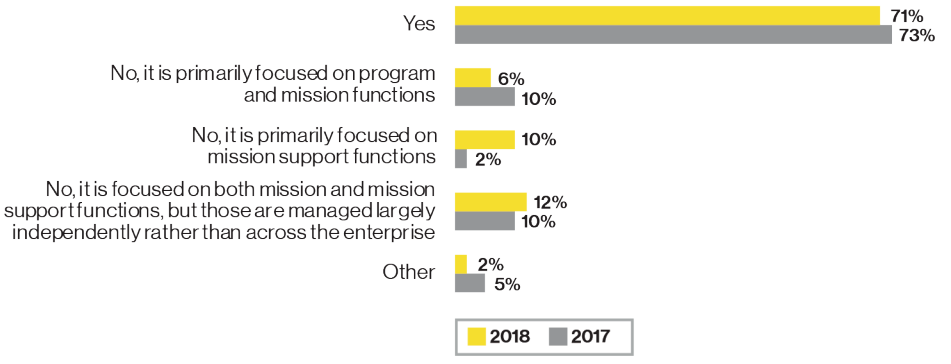
Nearly every organization with an ERM program has some form of an executive-level council to oversee the effort (93%), up 10% from the previous year. Just under half of the respondents (48%) indicate they have councils that monitor risk as it relates to strategy and performance. The rest focus on different aspects of risk, but not as comprehensive in terms of the relationship with strategy and performance. **Smaller organizations are more likely to have a comprehensive council that incorporates the relationship between risk with both strategy and performance** than the larger organizations represented in the survey (59% compared to 37%). The same breakdown exists for the longer duration ERM programs compared to the shorter duration programs (59% to 43%), as well as for ERM programs overseen by a CRO vs. all other ERM programs (65% to 38%).

Q: Do you have an executive-level council that reports and monitors risk as it relates to strategy and performance?



Beyond the role of the executive council, similar to last year **71% of respondents indicate that their ERM program is comprehensive, incorporating both mission and mission support activities** within its purview. The percentage goes up even further in some of our demographic breakdown areas. For example, 81% of smaller organizations report this kind of comprehensive ERM program, compared to 62% for larger organizations. The split is almost identical for longer duration programs (82%) compared to shorter duration programs (62%), and for ERM programs overseen by a CRO (83%) compared to all other ERM programs (62%).

Q: Is the focus of your Organization's ERM program comprehensive, encompassing a holistic view of mission and mission support functions?

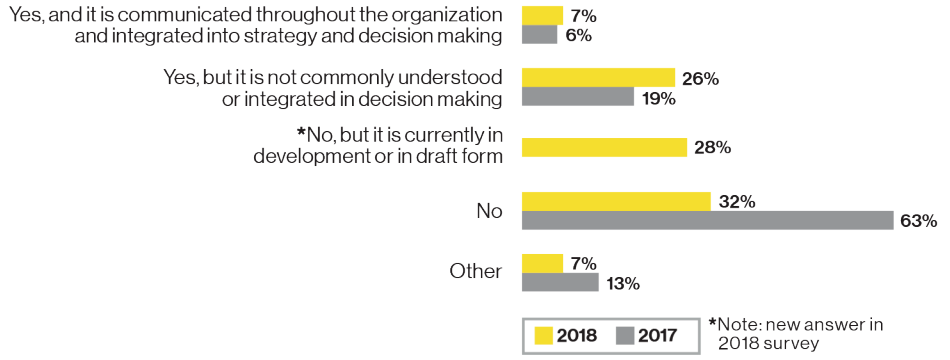


One of the elements of ERM that continues to be limited in adoption for Federal ERM programs is the concept of risk appetite. Similar to last year, **only 7% of respondents indicate that their organization has a defined risk appetite statement that is widely communicated and integrated into strategy and decision-making**.

One-quarter of respondents indicate having a risk appetite statement, but it is not commonly understood or not integrated in decision-making. Similar to last year, 60% indicate that they either do not have a risk appetite statement (32%) or it is still in development (28%). **Fewer than 10% of organizations across *any* of our demographic groups indicate having a well-understood and integrated risk appetite statement**.

That said, organizations with longer duration ERM programs are more likely to have *some* form of risk appetite statement (40%) compared to organizations with shorter duration programs (24%), and **organizations with an ERM program overseen by a CRO are nearly three times as likely to have a risk appetite statement** compared to organizations with an ERM program not led by a CRO (59% to 21%), even though many of these are neither well understood nor broadly used in decision-making.

Q: Does your Organization have a defined risk appetite statement?



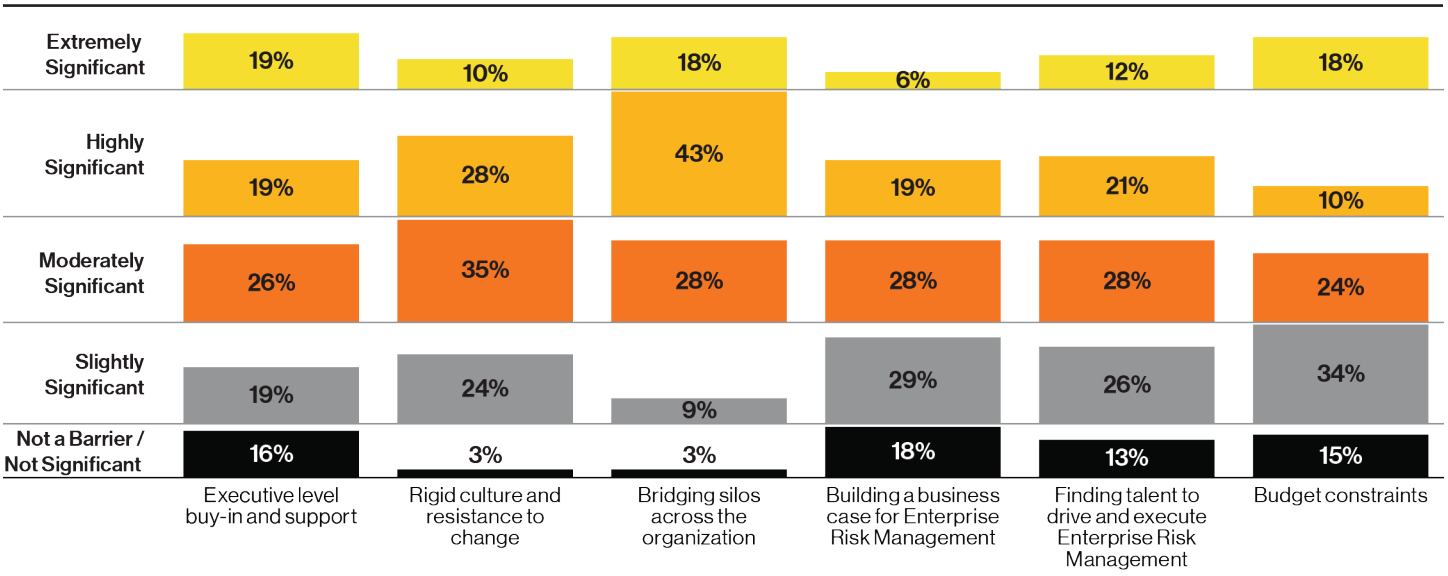
Motivations & Barriers

With its highest response rate in the four years of our survey (54% of respondents), **OMB Circular A-123 represents the primary motivator for the establishment of an organization's ERM program**. The desire for improved management decision-making is the only other motivator in double digits at 27%, the lowest level since the inception of the survey. Circular A-123 is the top motivator across every one of our demographic categories, with the **desire for improved management decision making a distant second in all categories**. In terms of those breakdowns, larger organizations and those that have established their ERM programs more recently have been more influenced by Circular A-123 than smaller organizations and the longer duration programs. The demographic comparisons show 69% of large organizations have implemented their ERM program primarily because of Circular A-123, compared to 38% for smaller organizations. That motivation holds for 59% of the shorter duration ERM programs, compared to 45% for the longer duration programs.

Q: Which of the following represents the primary motivator for the establishment of the Enterprise Risk Management program at your Organization?

The greatest barrier to establishing an ERM program continues to be "**bridging silos across the organization," topping our responses for the second straight year**, with 61% indicating that barrier as either highly significant or extremely significant. That characteristic is consistent across all of the demographic categories. "**Executive-level buy in and support" and "rigid culture and resistance to change" are next on the list, similar to last year**. The biggest change from the previous year is a drop in the area of "budget constraints" as a significant barrier, which was selected as a barrier by 50% of respondents last year compared to 28% this year who indicated a highly significant or extremely significant barrier. While all organizations share the most significant barrier of "bridging silos across the organization," those whose ERM program is not led by a CRO is approximately 50% more likely than the CRO-led ERM programs to face barriers such as "executive-level buy in and support," "rigid culture and resistance to change," and "finding talent to drive and execute ERM."

Q: Which barriers does your Organization face in establishing a formal Enterprise Risk Management program and how significant are those barriers? Please select the appropriate rating for each.

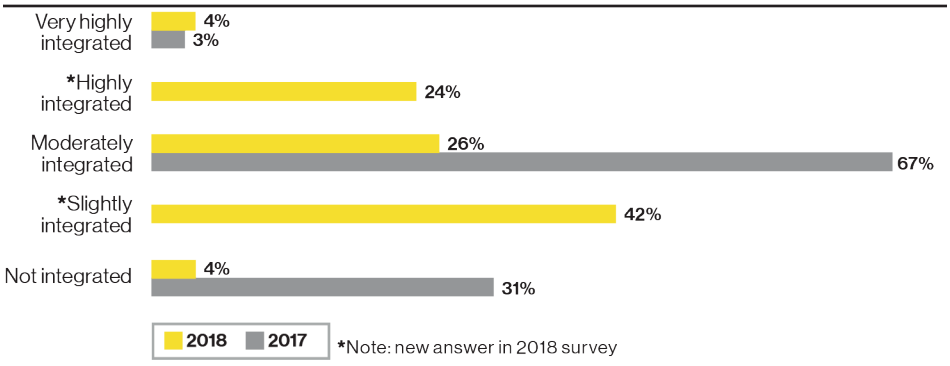


Integrated Capabilities

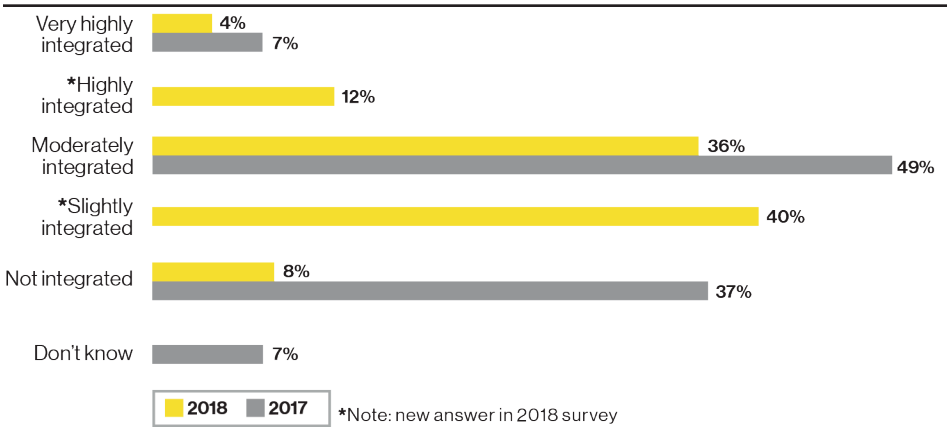
As noted previously, nearly half of our respondents indicate that their ERM programs are governed by an executive-level council that integrates risk with strategy and performance. However, **the degree to which Federal ERM programs are integrated with other discrete management processes is *much lower***. For example, the high levels of ERM integration (combination of "Highly" and "Very Highly" responses) peaks at just 28% in the area of strategic planning, followed by 16% for performance management and execution oversight, and 12% for integration with budgetary processes. When compared to the lower levels of integration (combination of "Slightly" and "Not Integrated"), there is nearly a **2-to-1 leaning toward lower levels of integration in the area of strategic planning** (48% to 28%). The differences are more pronounced for integration with the other processes. For example, in the area of ERM integration with performance management and execution oversight, respondents indicate their organizations are **three times more likely** to have a low level of integration (48%) than those in the high integration categories (16%). In terms of integration with budget processes, organizations are **five times more likely** to have a low level of integration (62%) than a higher level of integration (12%).

We also identified some stark differences in these areas of alignment in two demographic groups. Integration between these processes and ERM is much more prominent in longer duration ERM programs and organizations whose ERM program is overseen by a CRO, **although in *none* of these cases does the combination of Highly and Very Highly integrated top 50%**. Longer duration ERM programs compare much more favorably than shorter duration ERM programs in the categories of the higher levels of integration with strategic planning (34% to 25%), performance/execution processes (24% to 13%), and budgetary processes (24% to 4%). The differences are even more pronounced for organizations with CRO-led ERM programs compared to all others, with higher integration responses of 48% to 11% for ERM integration with strategic planning, 26% to 7% for performance/execution processes, and 22% to 4% for integration with budgetary processes.

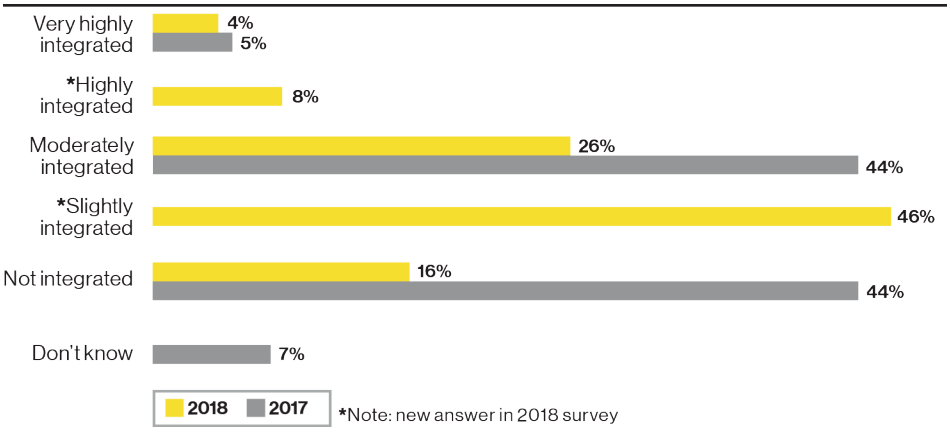
Q: To what extent has your Organization integrated Enterprise Risk Management into strategic planning?



Q: To what extent has your Organization integrated Enterprise Risk Management into execution processes (e.g., performance management and execution oversight)?



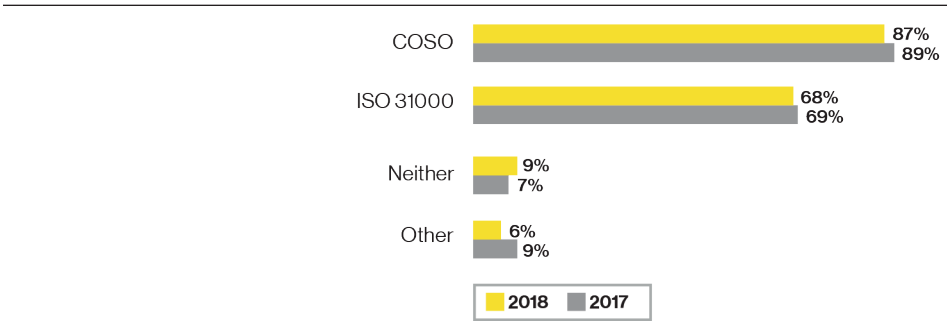
Q: To what extent has your Organization integrated Enterprise Risk Management into budgetary processes?



Industry Frameworks & Certification Programs

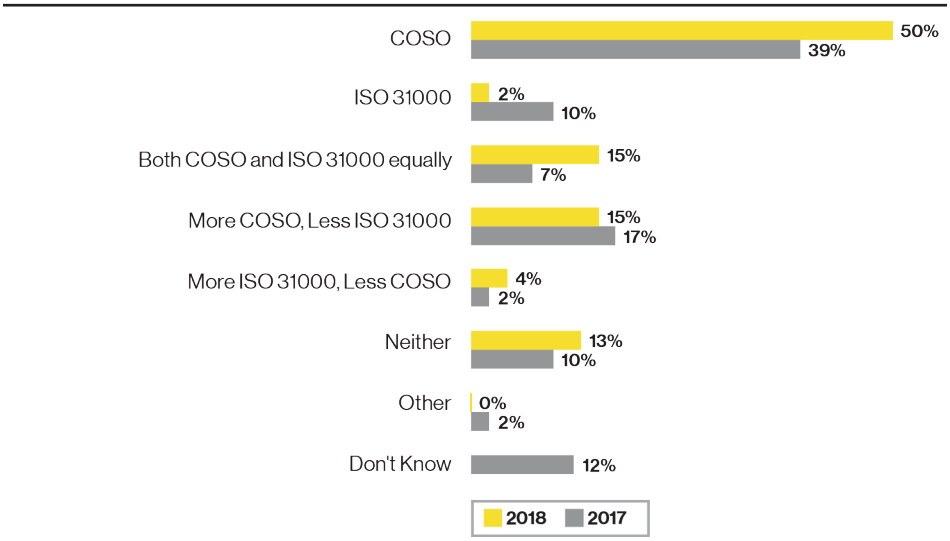
The COSO ERM Framework is the best known and most predominately followed in the Federal government for the fourth year in a row. Nearly **90%** of all respondents indicate familiarity with COSO, compared to 68% for ISO 31000.

Q: Which industry standard for Enterprise Risk Management are you aware of? Please select all that apply.



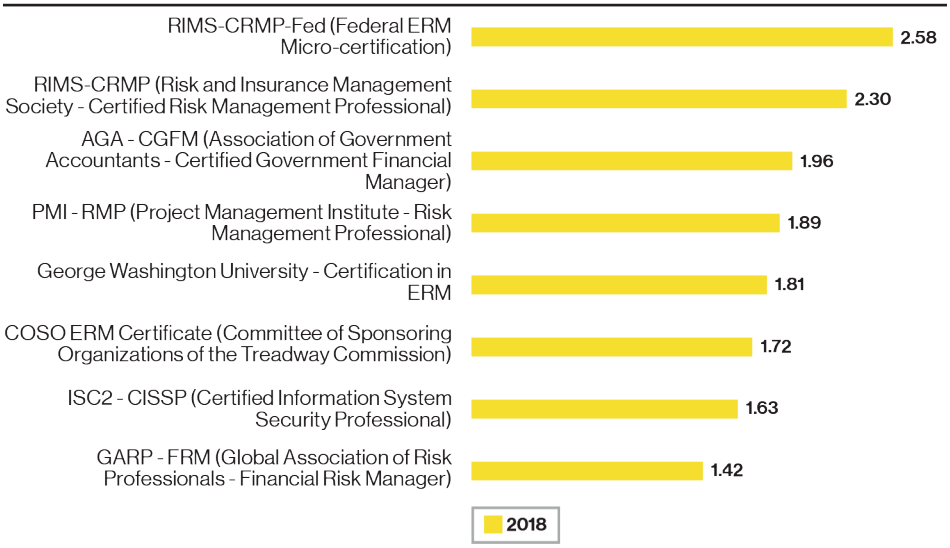
In terms of actual use, 65% of respondents indicate that their organization predominately follows COSO (50%) or More COSO, less ISO (15%). Only **2%** of organizations are using only the ISO ERM standard, with another 4% following More ISO, less COSO.

Q: Which industry standard for Enterprise Risk Management does your Organization predominately follow?



There are currently limited opportunities to pursue certifications specifically focused on ERM, and, until very recently, the opportunity to pursue a certification dedicated to *Federal* ERM was non-existent. To respond to this need, RIMS and AFERM introduced a first-ever Federal ERM micro credential earlier this year. **Of the eight risk management certifications listed in this year's survey, only two are perceived by our respondents as being either Moderately or Very Important, Useful, or Desirable: the Certified Risk Management Professional (CRMP) and the Federal Micro-Credential**, both from RIMS, each capturing greater than 50% of respondents in the two positive response categories. A majority of respondents indicate little to no awareness to most of the other credentials listed in the survey.

Q: What risk management or ERM certifications are you aware of and how important is it to you that you, your staff, or supporting contractors hold each certification? *(The results below represent the mean response for each type of risk exposure based on responses against a five-point scale.)*

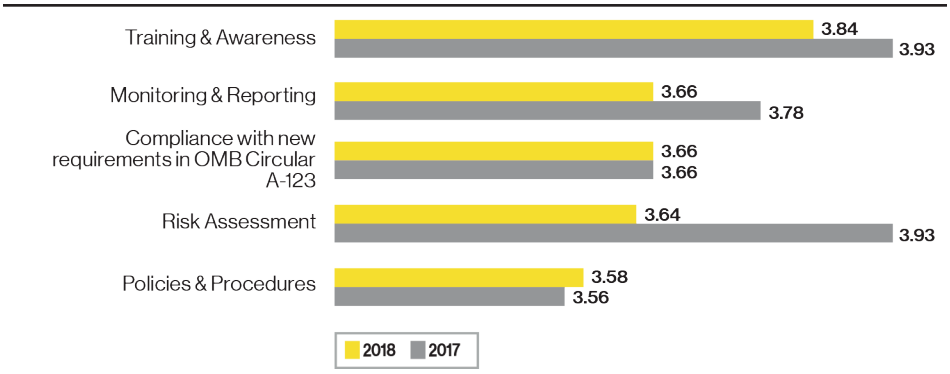


Focus & Priorities

For the second consecutive year, "Training & Awareness" represents the highest area of focus for current ERM programs over the next 12 months, which is further validated by survey responses in our section on ERM & Culture which indicate shortfalls in this area. There is very little variance this year from the highest area of focus to the lowest, with "Monitoring & Reporting" joining "Compliance with Circular A-123" just behind the top spot, followed closely by "Risk Assessment," and finally "Policies & Procedures." In terms of the demographic groups, focusing the next year's activity on "Compliance with Circular A-123" is highest amongst the larger organizations and lowest amongst the smaller organizations.

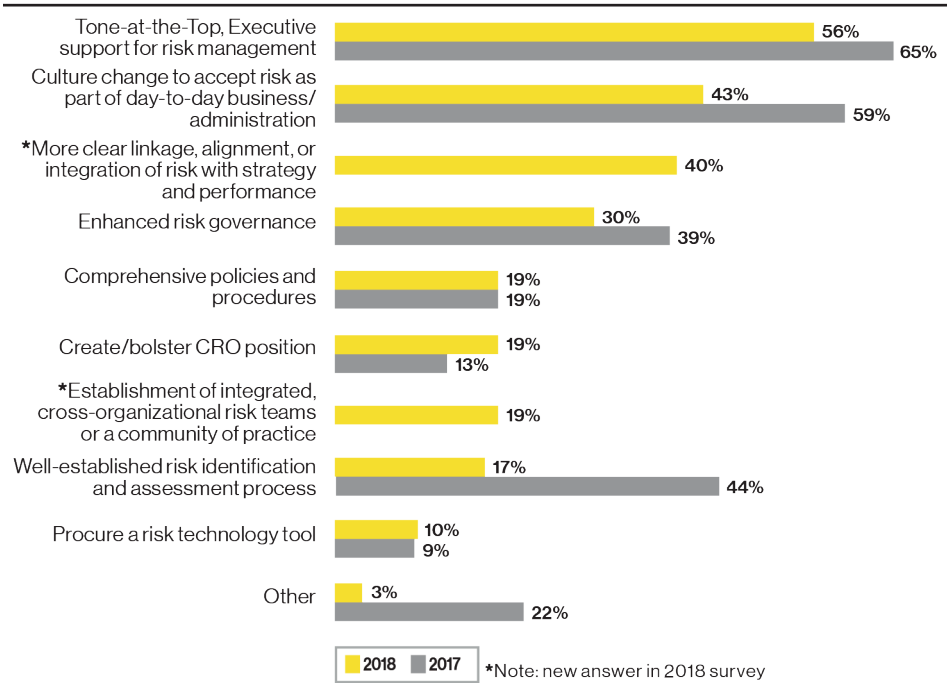
Focus & Improvement Opportunities for ERM Programs for the Next Year

Q: To what extent does your Enterprise Risk Management program plan to focus on each of the following over the next 12 months? *(Results are depicted showing the average score for each of the five choices listed from the following scale: (1) Decrease significantly; (2) Decrease somewhat; (3) No change; (4) Increase somewhat; and (5) Increase significantly. The higher average scores reflect greater focus in the next 12 months.)*



In terms of opportunities for improvement to enhance an organization's ability to respond to future risk scenarios, **three of the top four items remain the same as reported a year ago. "Tone-at-the-top, executive support for risk management" and "culture change to accept risk as part of day-to-day business/ administration" are #1 and #2 in this year's results**. A new category in this year's survey ("more clear linkage, alignment, or integration of risk with strategy and performance") appears in the #3 position, followed by "enhanced risk governance" which is #4 for the second straight year. **The biggest drop from last year is "well-established risk identification and assessment process**," which attracted only 17% of respondents this year compared to 44% a year ago. In the context of other aspects of this year's survey, it is noteworthy that "**create/bolster CRO position" continues to be one of the lowest priority areas for improvement** with only 19% of respondents selecting it from the list of options. **The lowest response rate continues to be "procure a risk technology tool**," generating only 10% of responses this year. Finally, organizations with non-CRO-led ERM programs are nearly twice as likely as organizations with CRO-led ERM programs to pursue "enhanced risk governance" as one of their most impactful improvement opportunities (37% to 22%).

Q: Please select the most impactful improvements that your Organization could make to be better positioned to respond to CURRENT and ANTICIPATED risks? *(The results below represent the mean response for each type of risk exposure based on responses against a five-point scale.)* Please select up to three.



Enterprise Risks

In this section, the focus and priorities for enterprise risks are explored from three perspectives:

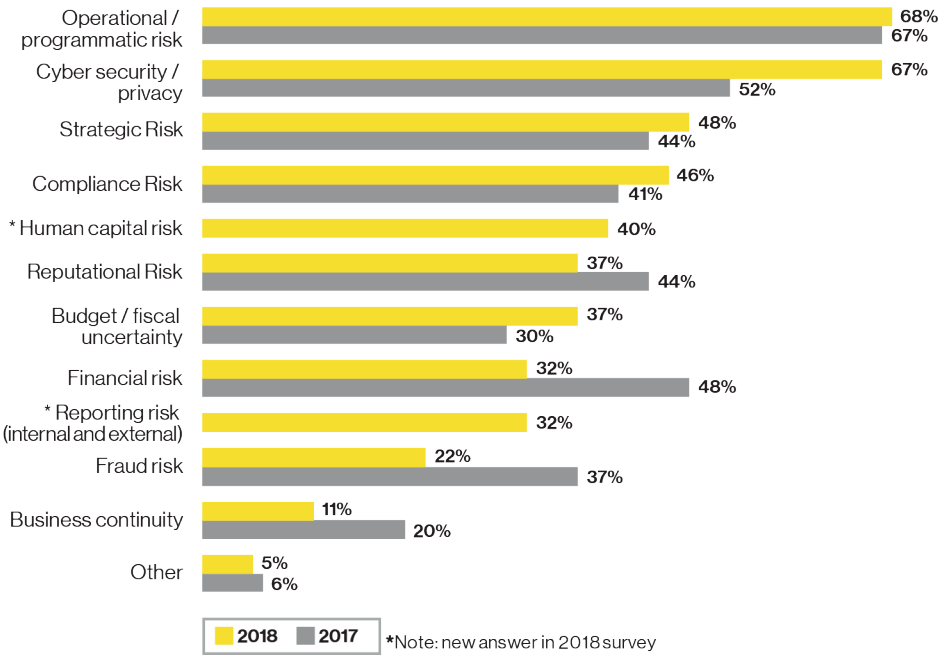
1. Management's current focus on risks
2. Perception of risks *currently* believed to have the greatest impact on the achievement of strategic objectives, regardless of management's focus
3. Perception of risks *anticipated* to have the greatest impact on the achievement of strategic objectives over the next 3-5 years, regardless of management's focus

Management's current focus on risks

Cited by a strong majority of 68% of respondents, **Operational Risk maintains the top spot for the second consecutive year as the type of risk that currently receives the greatest focus by management. Cyber Security/Privacy increased by 15 points compared to last year to narrowly miss the top spot at 67% of respondents**. Rounding out the top five are Strategic Risk, Compliance Risk, and Human Capital Risk (which was added as a new category for this year's survey). Business Continuity Risk fell to the bottom of the list at 11%, the lowest level in the four years of the survey.

We did identify some noteworthy differences amongst the demographic groups. For example, smaller agencies indicate a greater current emphasis by management on Reputational Risk compared to larger agencies (45% to 27%). On the other hand, larger organizations are spending more management attention on Budget/Fiscal Uncertainty compared to smaller organizations (47% to 27%). Organizations with CROs leading their ERM programs have the greatest management focus on Cyber Security/Privacy (83%), the highest of any demographic group. Organizations with CRO-led ERM programs are also focused extensively on Operational/programmatic risk (78%) and Compliance risk (65%).

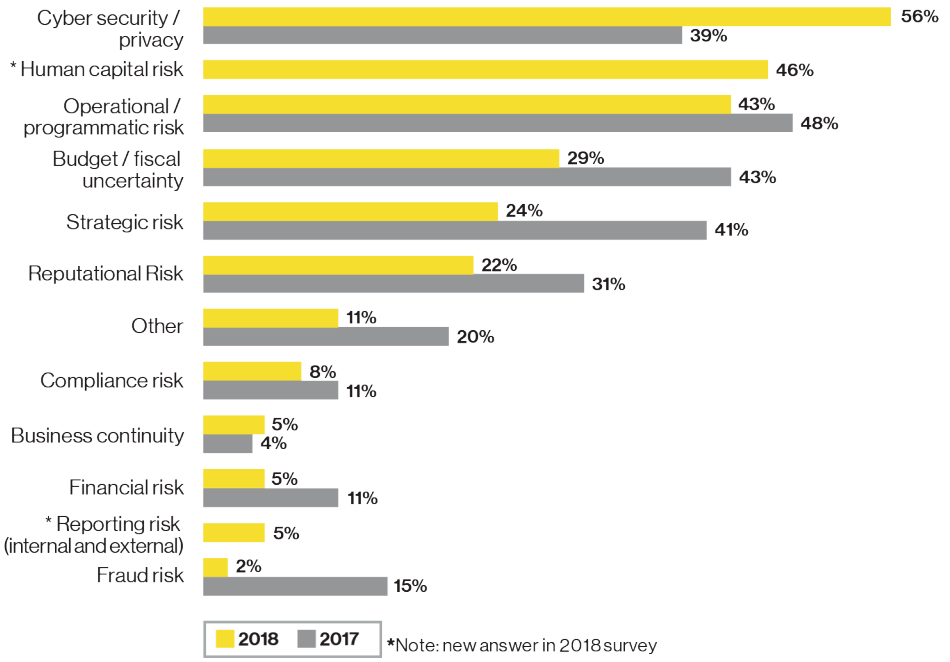
Q: Which types of risk does your management focus resources on the MOST? Please select all that apply.



Perception of risks *currently* believed to have the greatest impact on strategic objectives

Of the greatest risks organizations are facing regardless of current management's focus, **Cyber Security/Privacy topped the list at 56%**, followed by the new category of Human Capital Risk (46%) and Operational/Programmatic Risk (43%). **Several risks experienced significant decreases according to our respondents from the previous year, including Strategic Risk, Reputational Risk, Budget/Fiscal Uncertainty, and Fraud Risk**. Most of the demographic breakdowns were consistent with these overall results, although we do note that larger organizations are currently experiencing much greater perception of Cyber Security/Privacy Risk (70%) compared to smaller organizations (42%).

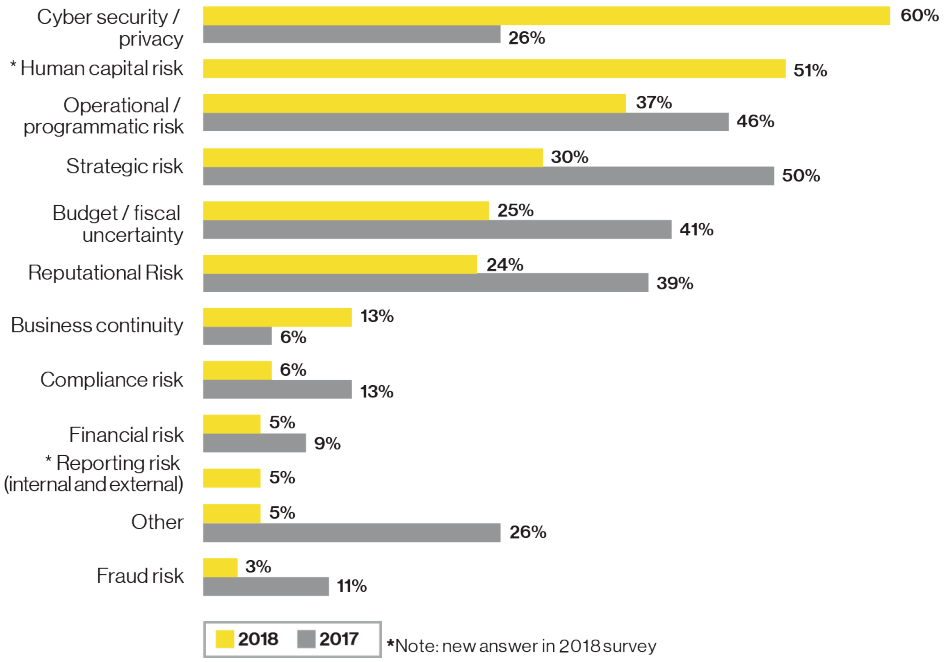
Q: Regardless of management focus, which types of risk are CURRENTLY perceived as the highest to your organization's ability to meet the mission or strategic objectives? Please select up to three.



Perception of risks *anticipated* to have the greatest impact on strategic objectives over the next 3-5 years

Sound risk management practices are always looking ahead to potential future risk events. This year, **Cyber Security/ Privacy is the top risk our respondents anticipate to have the highest impact on their organization in the next 3-5 years**, jumping nearly 35 points from the previous year to 60% this year. Human Capital Risk is second at 51%, followed by Operational/ Programmatic Risk (37%) and **Strategic Risk (30%). The Strategic Risk category fell by 20 points from the previous year**, dropping below 50% for the first time in the four years of the survey.

Q: Regardless of management focus, which types of risk do you ANTICIPATE to have the highest impact in the next 3-5 years on your organization's ability to meet the mission or strategic objectives? Please select up to three.



Comparison: Current Management Focus vs. Perception of Current and Future Risks

Summary: Top 5 by Category

The following tables summarize the top five results for each of the previous three questions.

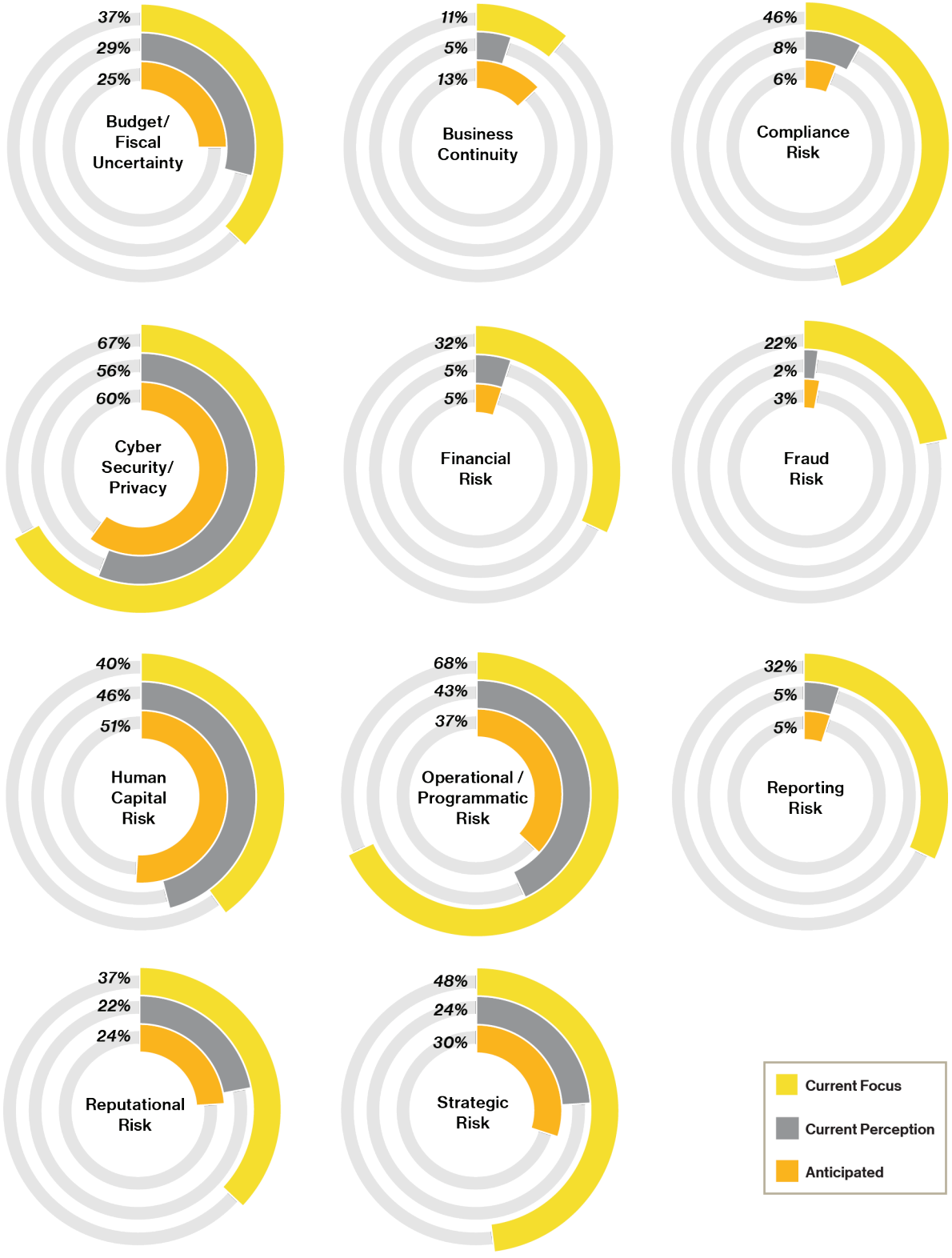
Management's Current Focus on Risks	Perception of Risks *Currently* Believed to have the Greatest Impact on Strategic Objectives	Perception of Risks *Anticipated* to have the Greatest Impact on Strategic Objectives over the Next 3-5 Years
1. Operational/ Programmatic Risk (68%)	1. Cyber Security/Privacy (56%)	1. Cyber Security/Privacy (60%)
2. Cyber Security/Privacy (67%)	2. Human Capital Risk (46%)	2. Human Capital Risk (51%)
3. Strategic Risk (48%)	3. Operational/ Programmatic Risk (43%)	3. Operational/ Programmatic Risk (37%)
4. Compliance Risk (46%)	4. Budget/Fiscal Uncertainty (29%)	4. Strategic Risk (30%)
5. Human Capital Risk (40%)	5. Strategic Risk (24%)	5. Budget/Fiscal Uncertainty (25%)

As can be seen in the "Top 5" listings above, there is high correlation across these categories for several risk types such as Cyber Security/Privacy which is consistently at the top of all three categories, indicating proper alignment between the perceived severity of the risk with the amount of management attention. Human Capital Risk is in the Top 5 in all three categories as well, but is ranked higher in both current and anticipated risks compared to how much management attention is currently being applied. Operational/Programmatic Risk also appears in the Top 5 across all three categories, albeit with a much higher depiction for the current receipt of management attention when compared to current and anticipated level of risk.

As can be seen on the following page, **some risk types are currently receiving significantly more attention from management compared to the perception of the current or perceived future risk** including the areas of Compliance Risk, Financial Risk, Fraud Risk, Reporting Risk, and Strategic Risk. For example, 46% of respondents identify Compliance Risk as receiving the most management attention, while only 8% of respondents perceive it as one of their organization's most significant risks and only 6% perceive it as one of their most anticipated future risks. Similarly, 22% identify Fraud Risk as receiving the most management attention, while only 2% perceive it as one of their organization's most significant current risks and only 3% perceive it as one of their most anticipated future risks. **These findings indicate a potential opportunity to reallocate resources that are currently being expended in these areas to focus on higher priorities and risks**, given the almost non-existent sense of actual current or future risks to their organizations.

Comparison: Current Management Focus vs. Perception of Current and Future Risks

(Note: Risks are listed in alphabetical order)



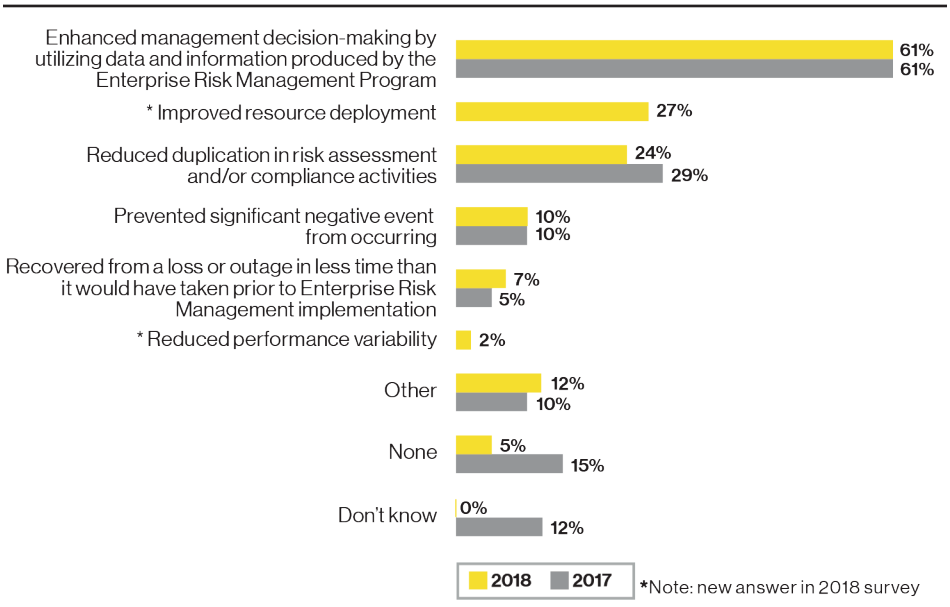
Execution & Performance

ERM Benefits

ERM programs exist to improve outcomes within organizations, but we also have seen over the years that these kinds of benefits can take a while to be realized. In that vein, this year's survey indicates very little change from the previous year in terms of the type and frequency of specific benefits being experienced by Federal organizations with an ERM program. Similar to last year, "**enhanced management decision-making" topped the list with 61% of respondents indicating such a benefit since the development of their ERM program.** However, also similar to last year, **no other benefit is evident for more than approximately a quarter of all respondents**. The new category, "improved resource deployment," is a benefit noted by 27% of respondents, followed by 24% selecting "reduced duplication in risk assessment and/or compliance activities." Very few other benefits are identified as being realized to date.

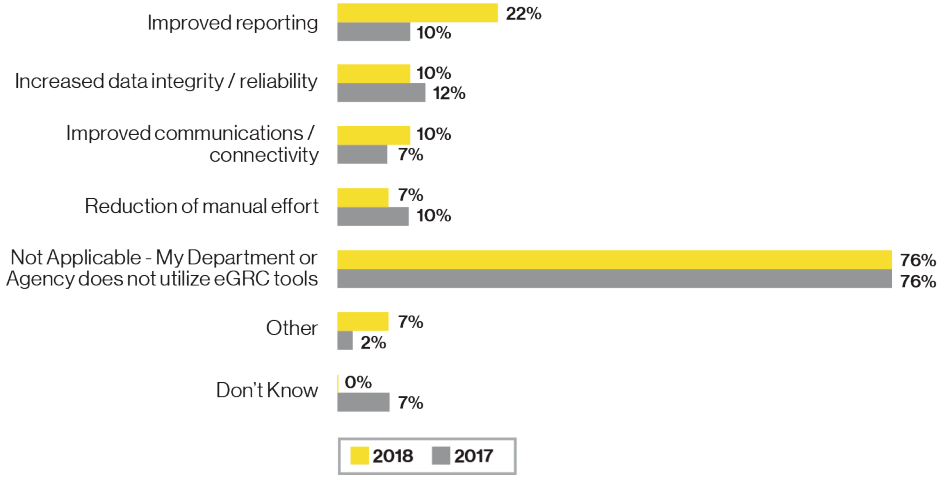
Longer duration ERM programs are more likely to realize just about all of the benefit options compared to shorter duration ERM programs. **Eighty percent of these longer duration programs have experienced "enhanced management decision-making**" (compared to 45% for the shorter duration programs). The longer duration programs indicate 35% experiencing "improved resource deployment," compared to 20% for the shorter duration programs. None of the programs which have existed for less than one year have realized just about any benefits to date. Organizations whose ERM program is overseen by a CRO indicate 73% have experienced "enhanced management decision-making," compared to 47% for all other organizations. **In the all-important category of "preventing a significant negative event from occurring," only 18% of CRO-led ERM programs indicate realizing this benefit, while none of the organizations with non-CRO-led ERM programs represented in this year's survey indicate realizing this benefit to date**.

Q: Since developing an Enterprise Risk Management program, which of the following benefits has your Organization realized? Please select all that apply.



We continue to see few benefits being realized by ERM programs resulting from the implementation of an enterprise Governance, Risk, and Compliance (eGRC) tool. The primary reason continues to be the lack of adoption of such tools in the Federal market, with **just over three-quarters of ERM programs indicating no such investment to date**.

Q: If your organization uses enterprise Governance, Risk, and Compliance (eGRC) tools, what benefits or returns has your Organization realized? Please select all that apply.

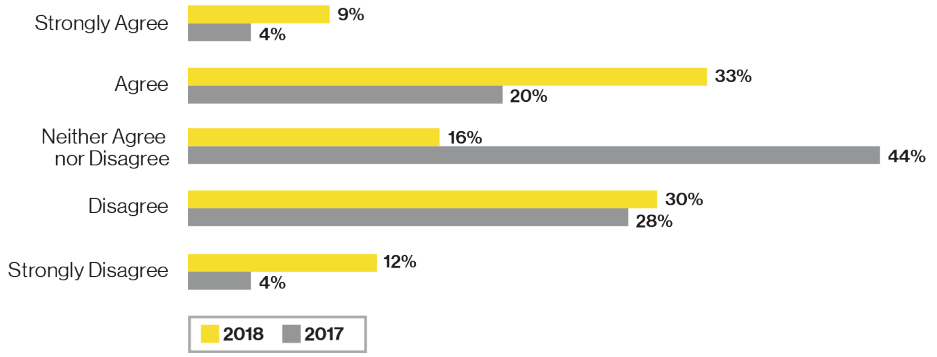


ERM & Culture

Earlier questions and analysis related to ERM & Culture highlighted some of the challenges confronting Federal organizations. To summarize, the survey portrays culture and leadership-related challenges as being the most prominent barriers facing organizations attempting to establish a formal ERM program ("bridging silos across organizations," "executive level buy-in and support," and "rigid culture resistant to change" as three of the top four items selected). In addition, the survey identifies "tone-at-the-top, executive support for risk management" and "culture change to accept risk as part of day-to-day business/administration" as the most impactful improvements organizations could make to better position themselves for current and anticipated risks. These observations (for both barriers and impactful improvements) are consistent across all demographic categories. The following five questions highlight additional characteristics of the nature of the cultural components of Federal ERM.

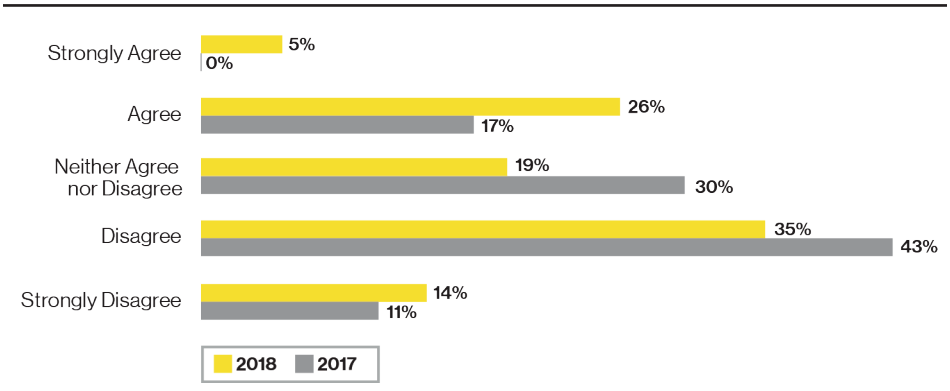
Management driving a culture of risk awareness through the tone at the top provides a balanced response with similar results at both the higher and lower ends of the responses. Approximately 42% of respondents indicate Strongly Agree or Agree, while a nearly identical 42% indicate Disagree or Strongly Disagree. The results are slightly better for organizations with longer duration ERM programs, **and much stronger for organizations whose ERM programs are run by a CRO** (64% to 29% in the case of the latter category's combination of Strongly Agree or Agree responses).

Q: In my organization, management drives a culture of risk awareness and openness through the tone at the top, which encourages employees to identify, report, and escalate potential risks.



For the second year in a row, organizations continue to fall short in providing sufficient risk management training to effectively and efficiently carry out their risk management responsibilities. **Only 31% of respondents indicate that their organization is providing sufficient risk management training (Strongly Agree or Agree). Organizations with longer duration ERM programs are far more likely than organizations with shorter duration ERM programs to provide sufficient training** (58% Strongly Agree or Agree compared to 23% for shorter duration programs). Moreover, **organizations whose ERM programs are overseen by a CRO are also more than twice as likely to provide sufficient risk management training than non-CRO-led ERM programs** (55% to 25% Strongly Agree or Agree).

Q: My organization provides sufficient risk management training for staff to effectively and efficiently carry out their risk management responsibilities.

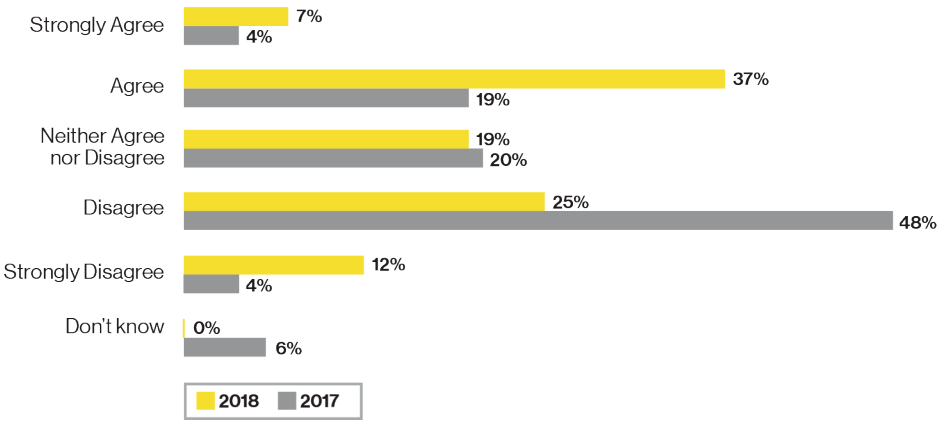


This year's survey indicates the strongest performance to date in the area of organizations embracing the cultural aspects of risk transparency, nearly doubling the results from previous years in the categories of Strongly Agree and Agree (44% compared to 23% in each of the previous two years). Placing the results on a 5-point scale results in a mean score of 3.02, **the only one of our culture-related questions that has a mean above the midpoint score** of 3.00. Two-thirds of longer duration ERM programs indicate Strongly Agree or Agree, compared to 44% for shorter duration ERM programs.

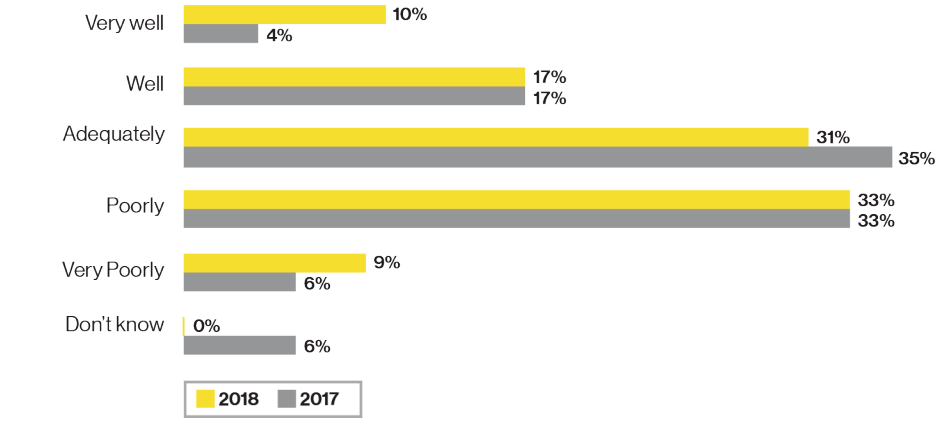
Despite a small uptick in results from last year, respondents still indicate that **their organization is more likely to *not* embed risk management as a component in all critical decisions** with 42% indicating this is done Poorly or Very Poorly in their organization, compared to only 27% for Well or Very Well. That said, these results flip for organizations with longer duration ERM programs compared to those with shorter duration ERM programs. For **organizations with longer duration ERM programs, 40% respond Well or Very Well and 80% indicate Adequately or above**. Organizations with shorter duration programs indicate 31% Well or Very Well.

Finally, ***very few* organizations are demonstrating alignment between their performance management system and their risk appetite**, encouraging the appropriate amount of risk taking in pursuit of their strategic objectives. Almost unchanged from a year ago, **only 16% of respondents answer affirmatively in this year's survey (combination of Strongly Agree and Agree) compared to 55% unfavorably (combination of Disagree and Strongly Disagree)**. These results are not surprising given the low adoption to date of well-understood enterprise risk appetite statements as revealed in an earlier question. The positive scores are low across all demographic categories, with the best result indicating just 27% on the high end for organizations whose ERM programs are overseen by a CRO, compared to 12% for all other organizations with ERM programs.

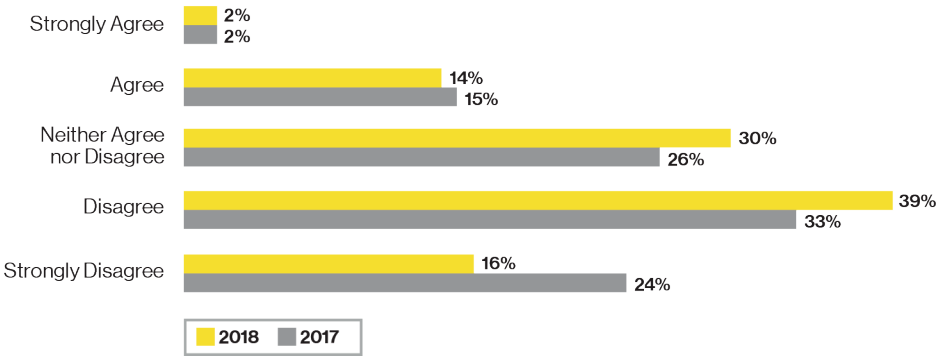
Q: My organization embraces the cultural aspects of risk transparency and promotes an environment where managers and staff are open to discussing risks as a part of everyday business.



Q: How do you rate how well your Organization seeks to embed risk management as a component in all critical decisions throughout the organization?



Q: My organization's performance management system is designed in alignment with my organization's risk appetite, and encourages an appropriate level of risk-taking in the pursuit of strategic objectives while maintaining accountability.

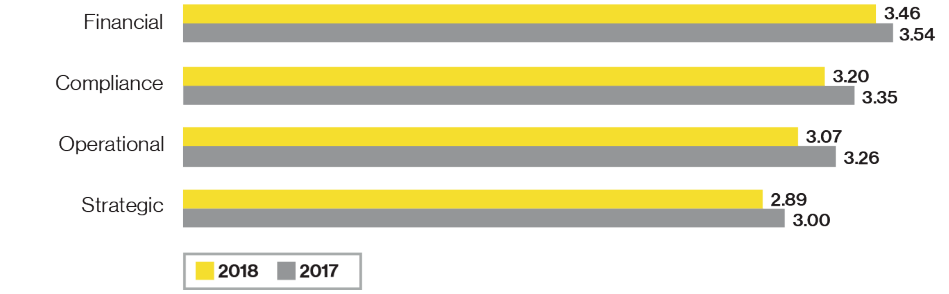


Performance Evaluation of ERM Capabilities

The following five survey questions all inquire about how well organizations with ERM programs perform in specific areas. For the first of these questions related to managing different areas of risk exposure, we provide the mean responses for each area. The other questions in this section all utilize the same 5-point scale (from Very Poorly to Very Well). Therefore we are able to calculate the mean response for each individual question. We present the mean result along with the bar chart with the full distribution of responses. **In each of these four questions, the mean result is less than the midpoint response of 3.00, and is lower than last year's mean score for three of the four questions. The results are stronger in each case for organizations with longer duration ERM programs and for organizations that have their ERM program led by a CRO**.

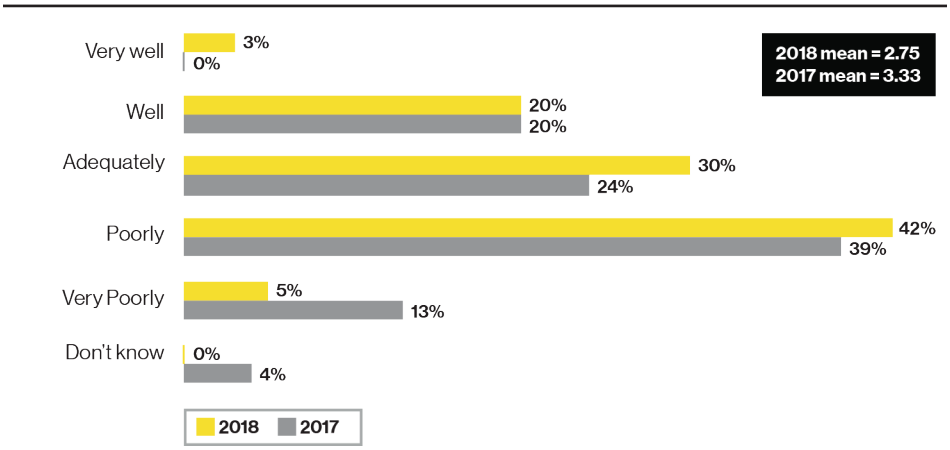
The order of proficiency in each of the four risk categories accounted for in this question remains the same as last year: (1) Financial, (2) Compliance, (3) Operational, and (4) Strategic. That said, **the average results were lower in all four risk areas when compared to last year's result**. Strategic Risk dipped below the midpoint response (3.00 on the 5-point scale) for the first time. **Organizations with longer duration ERM programs indicate higher results in all four categories**, when compared to organizations with shorter duration ERM programs, with the greatest differences in the areas of Strategic and Operational risk. **Organizations with CRO-led ERM programs are performing at a 15% to 20% higher rate for managing each of these areas of risk exposure (except Financial)** compared to organizations with non-CRO-led ERM programs.

Q: How do you rate how well your Organization manages all areas of risk exposure? *(The results below represent the mean response for each type of risk exposure based on responses against a five-point scale.)*



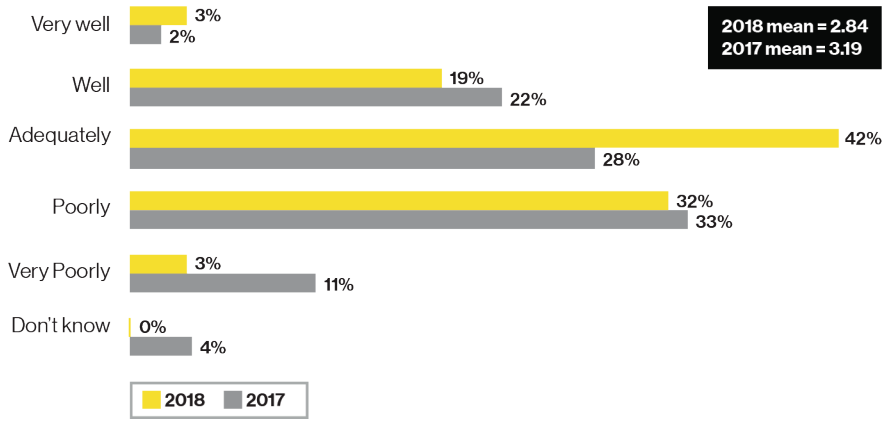
Prioritizing and managing risk across the organizational structure as an interrelated portfolio is the lowest performing in this section, with a mean result of 2.75. Organizations with longer duration ERM programs report results more than 40% better compared to organizations with shorter duration ERM programs (mean score of 3.48 for the former and 2.46 for the latter). Organizations with an ERM program led by a CRO demonstrate through the survey a 34% performance improvement in this area when compared to organizations with an ERM program not led by a CRO (mean score of 3.26 for the former and 2.43 for the latter).

Q: How do you rate how well your Organization prioritizes and manages risk across the organizational structure as an interrelated risk portfolio rather than within individual silos?



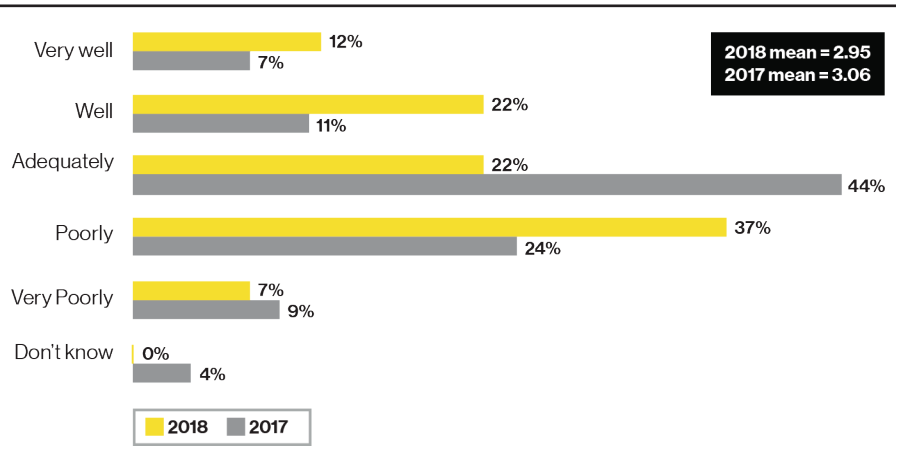
The overall mean response in the area of evaluating the risk portfolio in the context of all significant internal and external factors is slightly higher than a year ago, with a noteworthy movement of Very Poorly responses to an increase in Adequately responses. **The mean score for organizations with longer duration ERM programs is greater than 20% higher than for those with shorter duration ERM programs (3.29 to 2.72), with nearly identical results for organizations with CRO-led ERM programs compared to organizations with non-CRO-led ERM programs (3.30 to 2.70)**.

Q: How do you rate how well your Organization evaluates the risk portfolio in the context of all significant internal and external environments, systems, circumstances, and stakeholders?



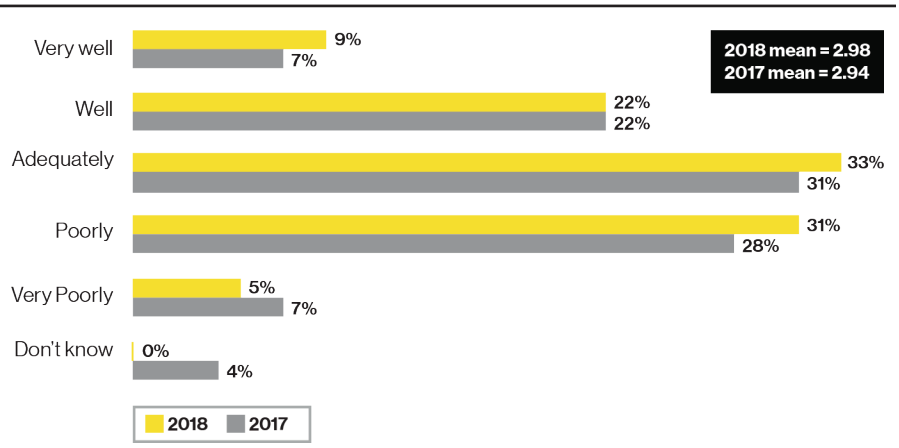
In terms of providing a structured process for the management of all risks, respondents indicate a move toward the more extreme responses, with a noteworthy increase from last year in the Very Well and Well categories, but an even greater increase in the Poorly and Very Poorly categories. The mean result of 2.95 falls just shy of the midpoint response of 3.00. Organizations with longer duration ERM programs produce a mean score just over 20% higher than organizations with shorter duration ERM programs (3.60 to 2.96). **The mean score for organizations with CRO-led ERM programs is more than 30% higher compared to organizations with non-CRO-led ERM programs** (3.70 to 2.79).

Q: How do you rate how well your Organization provides a structured process for the management of all risks?



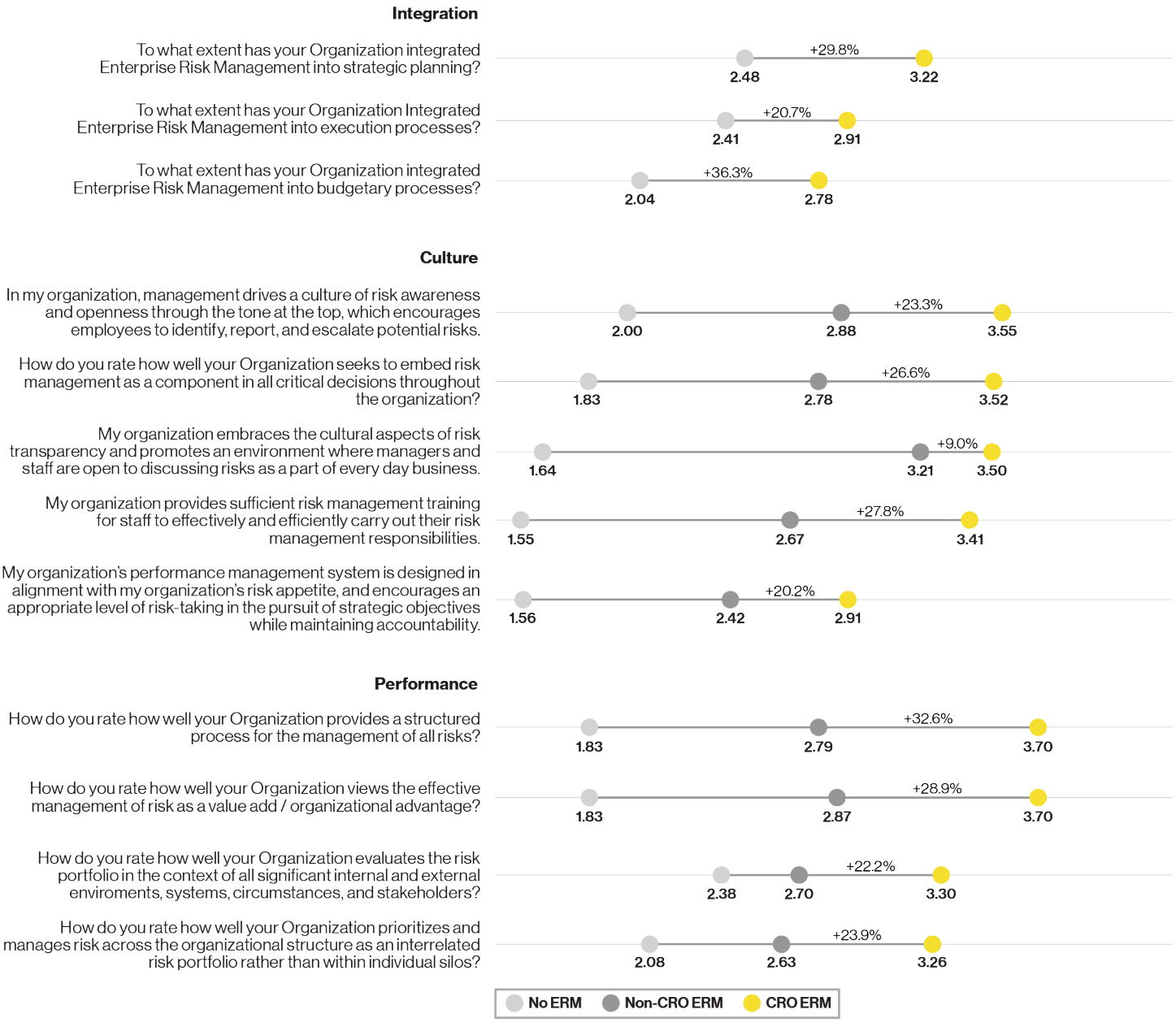
Viewing the effective management of risk as a value add/organizational advantage is the *highest performing* of the activities in this section as rated by our respondents, falling just shy of the midpoint response with a mean rating of 2.98. **The mean score for organizations with CRO-led ERM programs is more than 25% higher compared to organizations with non-CRO-led ERM programs** (3.52 to 2.78). This is the one question in this section which shows the least amount of difference between the mean results for organizations with longer duration ERM programs compared to organizations with shorter duration ERM programs (3.50 to 3.12).

Q: How do you rate how well your Organization views the effective management of risk as a value add / organizational advantage?

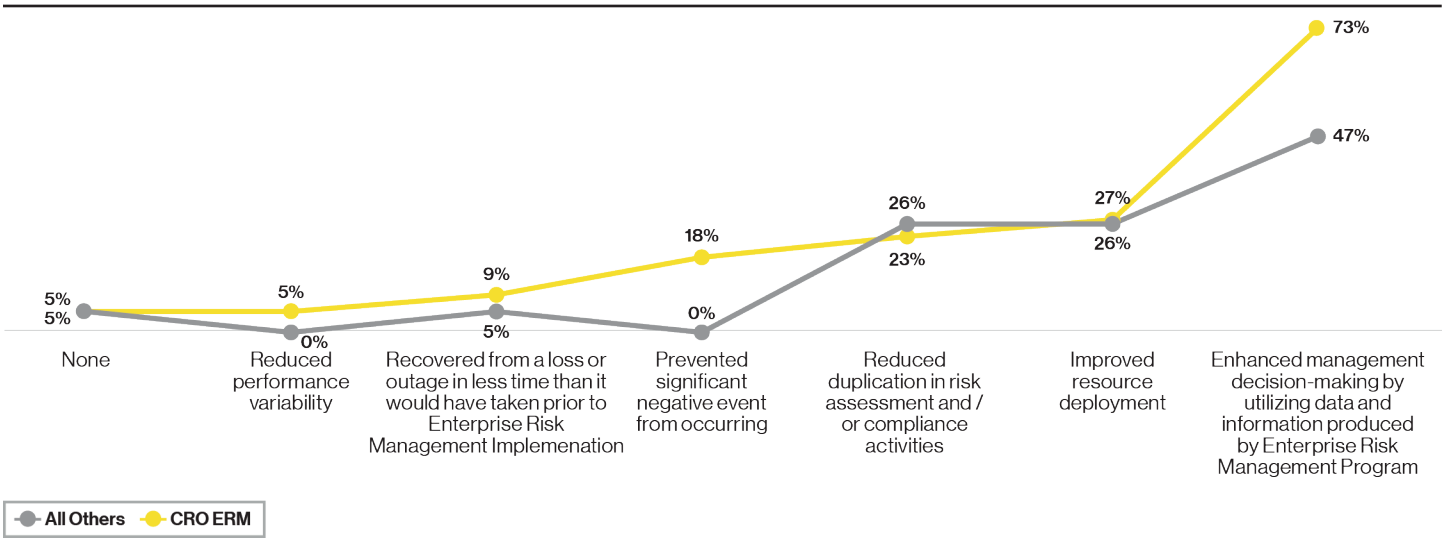


Chief Risk Officer Impact On Federal ERM Programs

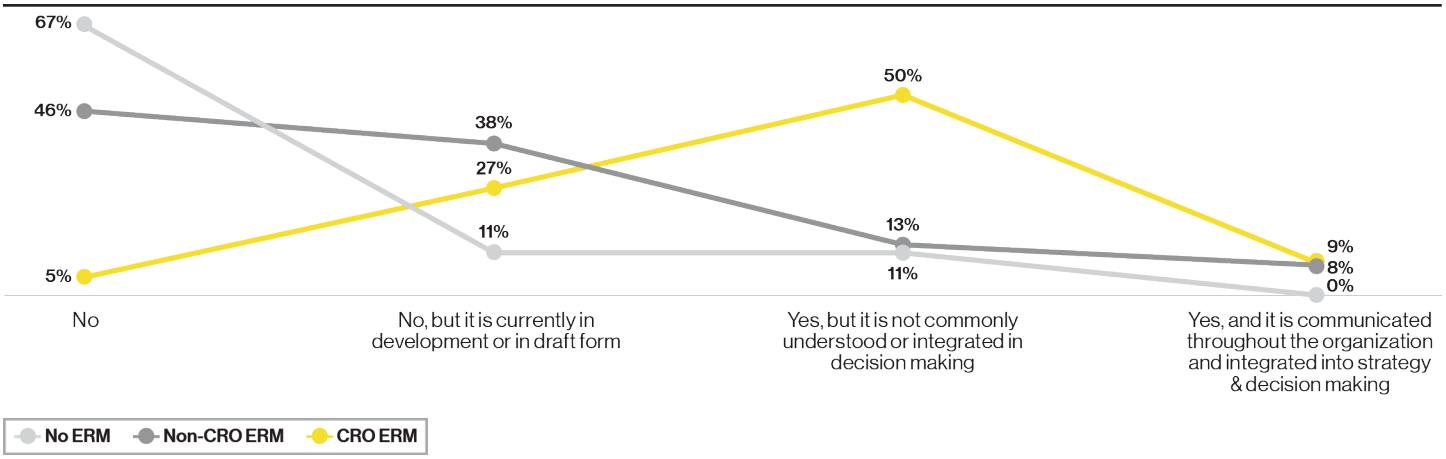
As highlighted in our Executive Summary, there is a clear trend in this year's survey depicting the positive impact that organizations are receiving when placing their ERM programs into the hands of a formal Chief Risk Officer. Almost without exception, organizational performance is enhanced, often significantly, for organizations with CRO-led ERM programs. The charts on this page and the next depict many of these results. In most of these cases, we highlight the mean responses (on a 5-point scale) from individuals who are in an organization where there is either No ERM Program ("No ERM"), in an organization where there is an ERM program not led by a CRO ("Non-CRO ERM"), and in an organization where there is an ERM program led by a CRO ("CRO ERM"). In previous surveys we have highlighted somewhat similar results when comparing performance for organizations with an ERM program vs. those without an ERM program, but this is the first year in which we identify noteworthy trends based on whether the leader of the ERM program is a CRO. The results are grouped by categories of questions, with the specific question on the Y-axis and the mean results presented to the right. The percentage improvement in the mean score is depicted as well.



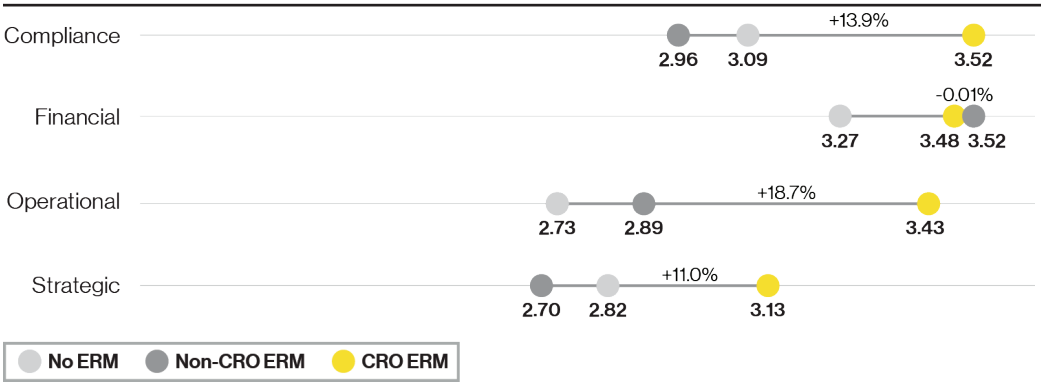
Q: Since developing an Enterprise Risk Management program, which of the following benefits has your Organization realized? Please select all that apply.



Q: Does your Organization have a defined risk appetite statement?



Q: How do you rate how well your Organization manages all areas of risk exposure?



About Us

Guidehouse

Guidehouse provides management, technology, and risk consulting to clients around the world through more than 1,600 professionals in over 20 locations. At our core, we focus on building trust in society, solving important problems, and having a seat at the table for our clients' most pressing matters. Formerly part of PwC, Guidehouse provides the exceptional quality our clients demand with the agility and innovation to go beyond the expected.

AFERM

AFERM is the only professional association solely dedicated to the advancement of Enterprise Risk Management (ERM) in the Federal government through thought leadership, education and collaboration. AFERM provides programs and education about benefits, tools and leading practices of Federal ERM and collaborates with other organizations and stakeholders to encourage the establishment of ERM in Federal departments and agencies. For more information about AFERM, please visit AFERM.org.

Award-Winning Excellence

In 2014, Guidehouse became the first large professional services firm ever to receive the nation's highest Presidential honor for quality - the Malcolm Baldrige National Quality Award. The Baldrige Award was established by Congress to recognize organizations for performance excellence through innovation, improvement and visionary leadership. Winning the award demonstrates Guidehouse's unparalleled commitment to quality and continuous improvement, which is embedded in everything we do and has enabled us to provide exemplary service to our Government clients.

Acknowledgments

This survey report is the product of a collaborative effort between Guidehouse and AFERM. We extend our gratitude to the respondents from the Federal ERM community to our online survey. Our analysis and reporting would not be possible without your time and candid input.

Primary Contributors

Guidehouse

www.guidehouse.com

David Fisher
dfisher@guidehouse.com

Cameron Arimoto
carimoto@guidehouse.com

AFERM

www.AFERM.org

Peggy Sherry
president@aferm.org

Tom Brandt
president@aferm.org

Sallyanne Harper
saharper1@Verizon.net

Additional contributions

Kate Sylvis

Sarah Choi

Karl Keiffer

Nelly Singla

Marketing

Christina Vanecek

Creative

Angela D'Agostino

Contacts

For more information, please contact:

David Fisher
Managing Director
Public Sector Risk Consulting Leader
dfisher@guidehouse.com
(571) 251-2260

Tom Brandt
President-Elect
Association for Federal Enterprise Risk Management
president@aferm.org