www.pwc.com/federalERM

Federal Enterprise Risk Management

2017 Survey Results

The 2017 ERM survey is PwC's third annual survey performed in collaboration with the Association for 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

pwc

Executive Summary

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

This year's survey continues to demonstrate the year-over-year trend of new ERM programs coming into existence across the Federal government, many of which still exhibit capabilities that are predominately in the early stages of development, particularly with respect to the cultural and leadership aspects of effective ERM.

Last year's survey report characterized Federal ERM as a "start-up industry." That depiction remains valid. **While ERM programs continue to emerge and grow across the Federal government, these programs generally find themselves in the initial stages of the development life cycle when viewed in context of the full spectrum of ERM capabilities.**

As a summary, here are some of the most significant insights stemming from this year's survey:

Top 10 Findings

- The past year witnessed a jump of approximately 50% in the total number of ERM programs in the Federal government compared to last year's survey, with nearly half of this year's respondents working in organizations with ERM programs that are less than one year old.
- OMB Circular A-123 re-emerged as the top motivator for Federal ERM programs this year, barely eclipsing "Desire for improved management decision-making" which was last year's number one motivator.
- Cultural and leadership aspects of ERM are identified as both primary barriers for establishing ERM programs and areas with the greatest opportunity for improvement, more significant than processes, procedures, and technology. "Bridging silos across organization" is identified as the top barrier, selected by 85% of survey respondents.
- A strong majority of Federal ERM programs do not have risk appetite statements, and even those that are in place are rarely used to effectively guide decision-making.
- ERM integration with processes related to strategy, budget, and execution/performance is very limited across Federal ERM programs.
- There is a fairly significant misalignment between the risk areas currently receiving management's greatest attention and those risks perceived to represent the greatest potential impact on the achievement of strategic objectives, both currently as well as anticipated over the next 3-5 years.
- Benefits continue to be realized from Federal ERM programs, particularly in the area of enhanced management decision-making, but the overall depiction of benefits is less than those provided by last year's respondents. This result appears to be influenced by the introduction of so many new ERM programs this year, nearly half of which indicate receiving no benefits thus far in their short tenure.
- Most of the cultural aspects of ERM (e.g., risk transparency, tone-at-the-top, bridging organizational silos, and commitment to training) remain generally immature capabilities with below average ratings from survey respondents.
- A number of other ERM program performance measures (e.g., ones related to structured processes, the use of ERM for organizational advantage, and taking a holistic view of risk) receive more favorable results compared to the cultural aspects of ERM, but are still generally below average among the choices offered.
- ERM technology, specifically enterprise Governance, Risk, and Compliance (eGRC) tools, remains a low priority with a low rate of adoption for Federal ERM programs.

Report Organization

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

- Characteristics of Federal ERM Programs
- Focus & Priorities
- Execution & Performance

Subsections are included for each category, including a new section on ERM & Culture that is introduced under Execution & Performance. In context of these categories, the results from this year's survey responses are provided, along with comparison results from the from 2015 and 2016 surveys, as appropriate. 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
PwC Public Sector
Risk Consulting
Leader

Sallyanne Harper
President
Association for
Federal Enterprise
Risk Management
(AFERM)

Contents

Survey Approach & Demographics

This report provides the results of the third annual survey conducted by PwC 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. A few questions included in last year's survey were eliminated due to overlap with other questions and a small number of new questions were introduced to address potential new trends, particularly in the area of the cultural aspects of ERM in the Federal government. The report's bar charts include data from the 2015, 2016, and 2017 surveys, except in the case of the few new 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 19 and August 18, 2017. Links to the online survey were sent to all 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 or not 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 25 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.

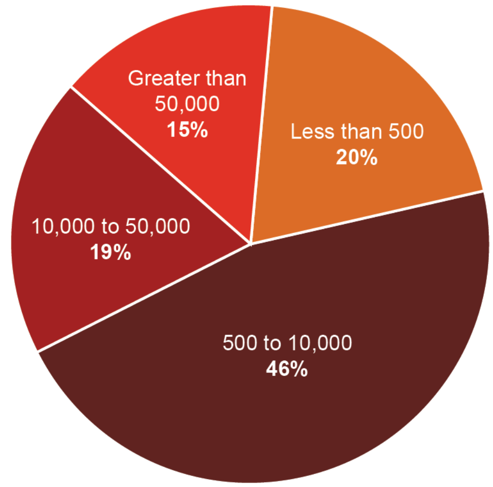
The 25 organizations from which responses were received include the following (in alphabetical order):

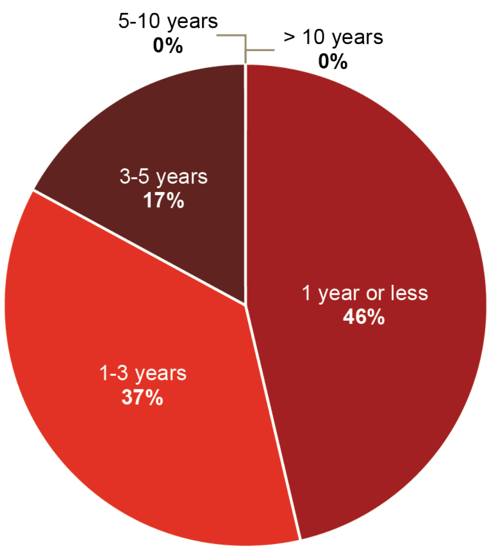
- Architect of the Capitol
- Consumer Financial Protection Bureau
- Corporation for National and Community Service
- Department of Commerce
- Department of Defense
- Department of Health and Human Services
- Department of Homeland Security
- Department of Housing and Urban Development
- Department of Justice
- Department of State
- Department of the Interior
- Department of the Treasury
- Department of Transportation
- Export-Import Bank of the U.S.
- Federal Energy Regulatory Commission
- Federal Trade Commission
- Millennium Challenge Corporation
- National Archives and Records Administration
- National Credit Union Administration
- National Endowment for the Arts
- National Science Foundation
- Securities and Exchange Commission
- Small Business Administration
- United States Postal Service
- Veterans Administration

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 some 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"** (66% of respondents, less than 10,000 employees) while the two largest response categories are combined and referred to as **"larger organizations"** (34% of respondents, more than 10,000 employees).





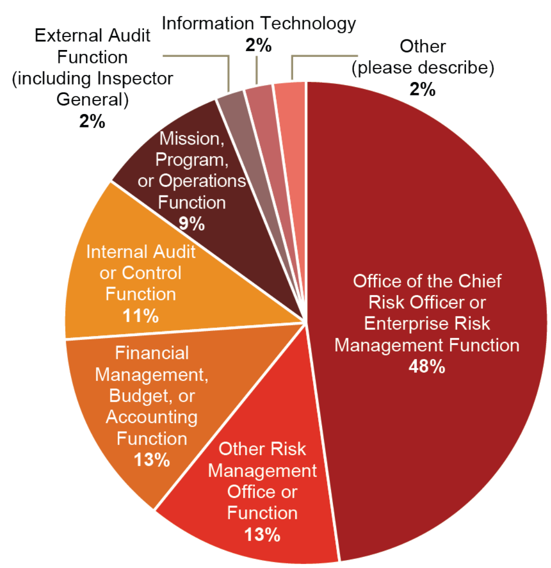
How long has your Organization practiced ERM?

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"** (83% 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"** (17% 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 active ERM program.

Current functional alignment within your Organization.

To simplify the analysis associated with the functional alignment of the survey's respondents, the two functions specifically related to risk management are combined in the narrative portion of this document and referred to as **"risk management functions"** (61% of respondents) while the responses related to any other functional area are combined and referred to as **"non-risk management functions"** (39% of respondents).



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

Survey Results

Characteristics of Federal ERM Programs

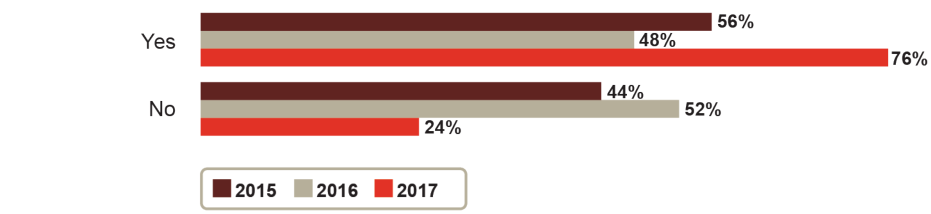
ERM Existence, Duration, & Size

The Federal ERM community continued to expand in 2017, **with more than three-quarters of respondents indicating that their organization has an existing ERM program, an approximately 50% increase from the previous two years.** Many of those programs have, in fact, been newly established. **Nearly half of the ERM programs identified in the survey have been in existence for one year or less, and more than 80% have been in existence for three years or less.**

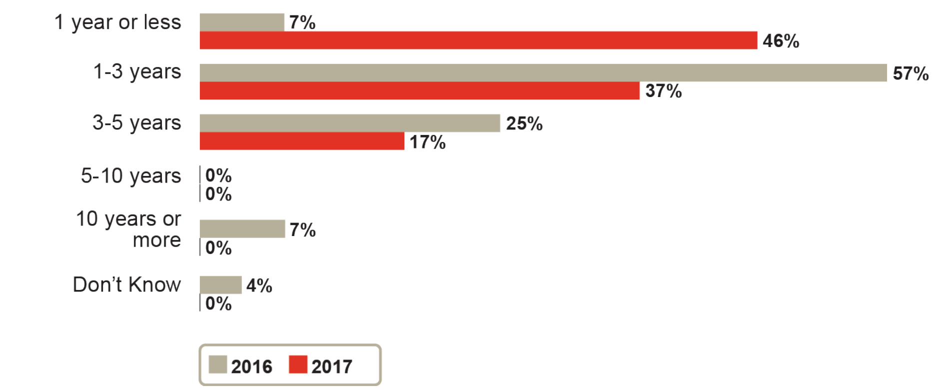
In terms of differences amongst the demographic breakdowns, larger organizations have typically had their ERM programs for longer durations. Specifically, almost half of the larger organizations that responded to the survey indicate they have had their ERM program for longer than three years, compared to only 4% of the smaller organizations having ERM programs in place for that duration. Readers will note that previous surveys included a very limited number of organizations that had ERM programs for longer than five years. While those programs continue to exist, no data was received for this year's survey from organizations whose ERM programs fit that demographic category.

ERM programs continue to be relatively small operations in terms of both manpower and financial resources. Similar to the last two years, just under 60% of Federal ERM programs maintain a staff of 5 FTE or less (including contractors) and 86% have less than 10 FTE. At the demographic level, smaller organizations and organizations with shorter duration ERM programs tend to have smaller headcount in their ERM function. These contrast with larger organizations and those with longer duration ERM programs, both of which tend to be slightly larger.

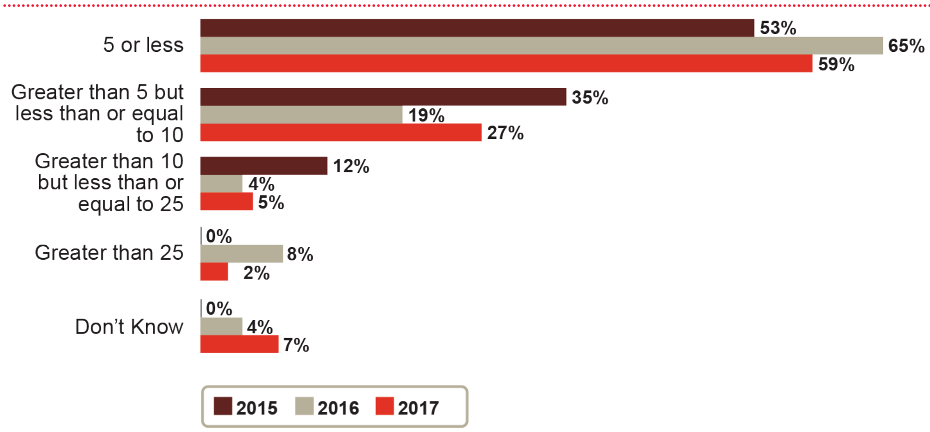
Q: Does your Organization have a formal Enterprise Risk Management program?



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



Q: How many full time equivalents (including contractor support) are working in the Enterprise Risk Management function?

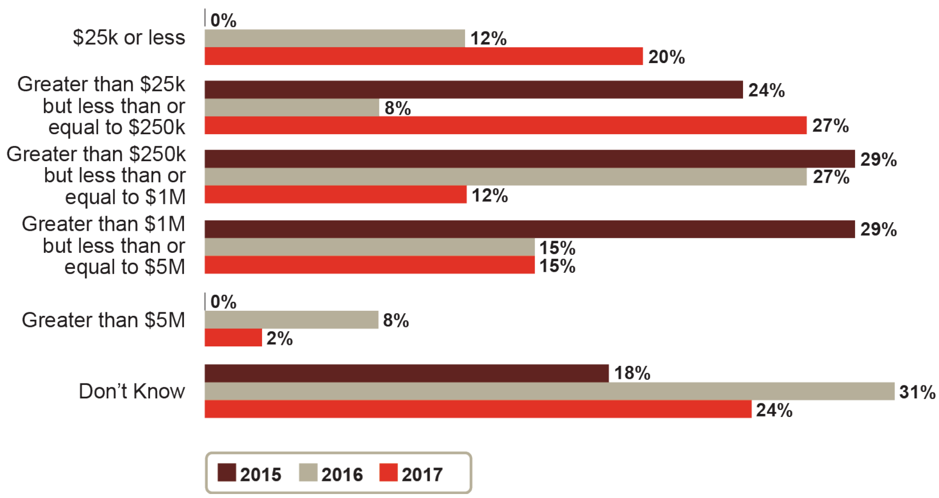


The pattern for financial resources is similar to that of human resources in that Federal ERM programs maintain relatively small budgets. **Nearly 60% of these programs have budgets less than $1 million** (slightly higher than last year). The larger organizations and those with longer duration ERM programs tend to have larger budgets than those in smaller organizations or with shorter duration ERM programs. For example, **just over 50% of the shorter duration ERM programs have budgets less than $250,000 and only 10% of those programs have budgets over $1 million.** In contrast, none of the longer duration ERM programs have budgets less than $250,000, and nearly 60% have budgets over $1 million.

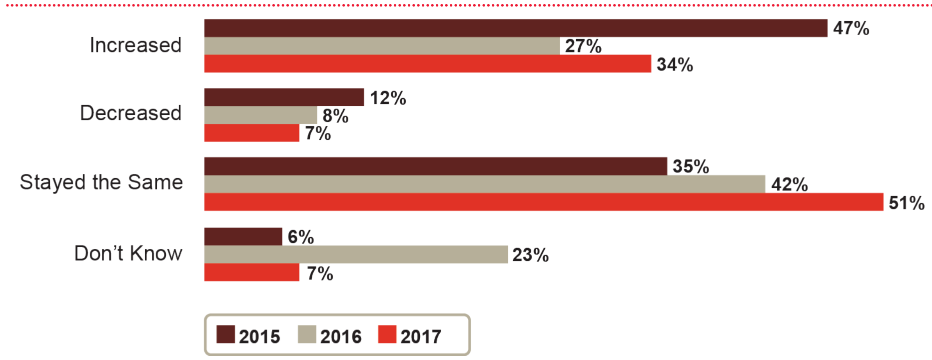
In terms of budget trends, about a third of Federal ERM programs indicate an increase in budget over the previous year, while about half saw no change in year-over-year budget. For the demographic breakdowns, nearly half of smaller organizations experienced a budget increase for their ERM program in the past 12 months, while none saw a decrease. This compares to ERM programs in larger organizations which experienced little change in budgets in about 60% of cases from the previous year, but also had budget decreases for nearly a quarter of these organizations during the same period. **The greatest budget pressure appears to be in those organizations where an ERM program has existed for more than three years.** None of these longer duration ERM programs indicate a budget increase from the previous year, while nearly 30% experienced a budget decrease.

In terms of evidence of expectations of demand for effective ERM activities, the survey once again indicates **a strong expectation of continued increased demand (80% responding affirmatively)**, acknowledging that while this continues to be an incredibly high expectation it is slightly lower than either of the two previous years. The two demographics indicating the greatest expectation for increased evidence of effective ERM activities are larger organizations (95%) and those with the longer duration ERM programs, where the sentiment is unanimous.

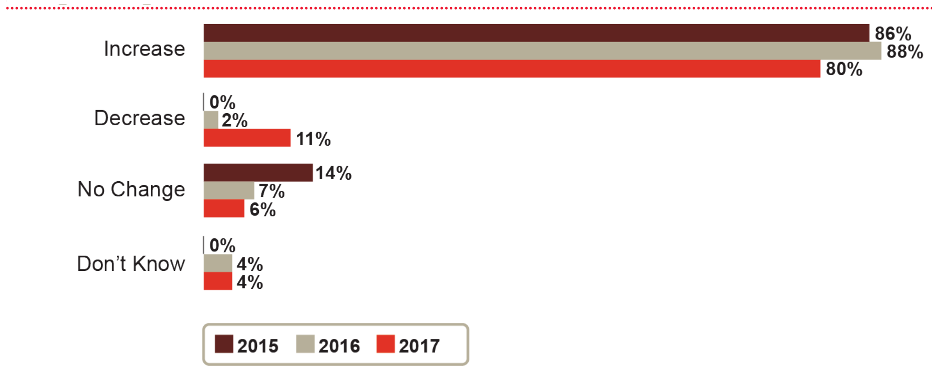
Q: What is the total annual budget for Enterprise Risk Management activities across your Organization?



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



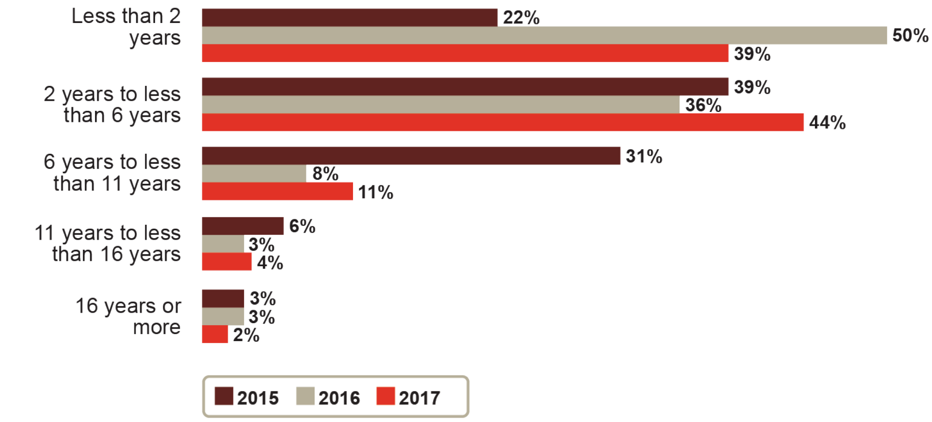
Q: Do you believe the demand for evidence of effective Enterprise Risk Management activities will increase or decrease over the next three years?



Tenure & Titles

As part of the emerging nature of ERM in Federal organizations, the tenure in risk management roles remains relatively low. Nearly 40% of all survey respondents indicate that they have been in their current position less than two years. For people in risk management functions, that percentage edges up close to 50%, compared to around 30% for respondents who work outside of the risk management domain.

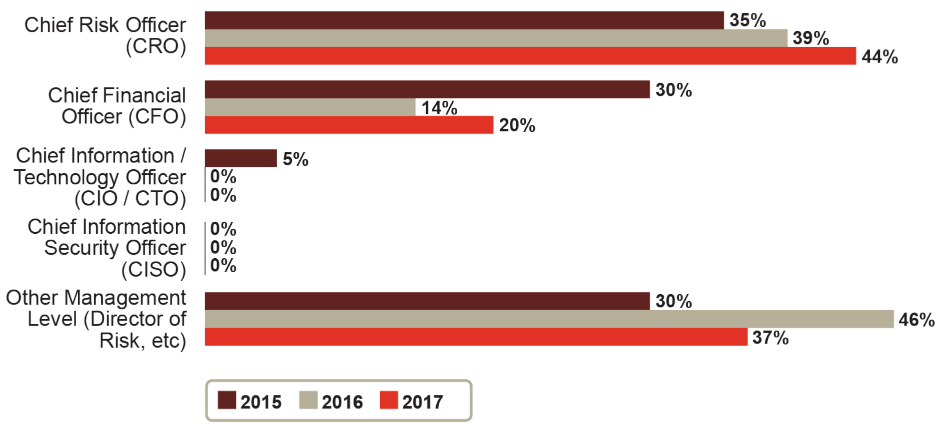
Q: How many years have you served in this position (all survey respondents)?



In terms of leadership positions and titles, this year's respondents indicate that **Chief Risk Officers (CROs) are slightly more prominent in Federal organizations compared to the responses from last year's survey** (44% this year compared to 38% a year ago). Longer duration ERM programs are nearly twice as likely to have a CRO in place than shorter duration ERM programs (71% to 38%). Also, larger organizations have embraced the position of CRO in more than half the cases (54%) compared to 39% for smaller organizations.

The second position to lead Federal ERM programs remains the Chief Financial Officer (CFO) at 20% response, representing less than half than those with a CRO in the lead position. A little more than a third of respondents indicate ERM leadership with a title not among the choices provided, portraying a degree of organizational variability for ERM across the Federal government.

Q: Which of the following titles best describes the person responsible for your Organization's Enterprise Risk Management program? If other, please elaborate.

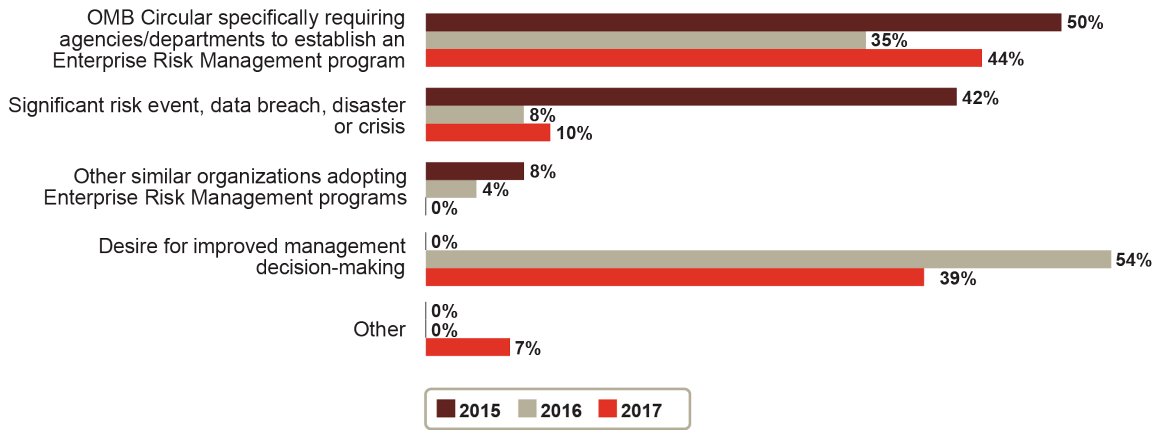


Motivation & Barriers

The *motivation* for the establishment of an ERM program in Federal organizations has shifted over the past couple of years. In 2015, anticipation of new requirements in OMB Circular A-123 dominated this motivation, but that was eclipsed last year by the desire for more improved management decision-making. **This year, requirements in OMB Circular A-123 re-emerged as the top overall motivator for the establishment of an ERM program (44% of respondents), slightly ahead of the desire for improved management decision-making (39%).**

That said, there is significant variability on motivation based on the characteristics of the organization and personnel. For example, similar to last year, OMB Circular A-123 is cited as the top motivator by 50% of both smaller organizations and organizations with shorter duration ERM programs. For ERM programs established in the past 12 months, Circular A-123 was cited as the top motivator for the program by 63% of respondents, the most by any demographic breakdown. That number slips to 30% for larger organizations, and to 14% for organizations with longer duration ERM programs. Responses also vary considerably among people who reside in risk management functions compared to those who work in other business areas. OMB's A-123, for example, is cited as the top motivator for establishing an ERM program by only 32% of risk management personnel, but that figure more than doubles to 69% for non-risk management staff. Moreover, **desire for improved management decision-making is the top motivator for more than half of risk management personnel (54%), compared to only 8% for non-risk management staff.**

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

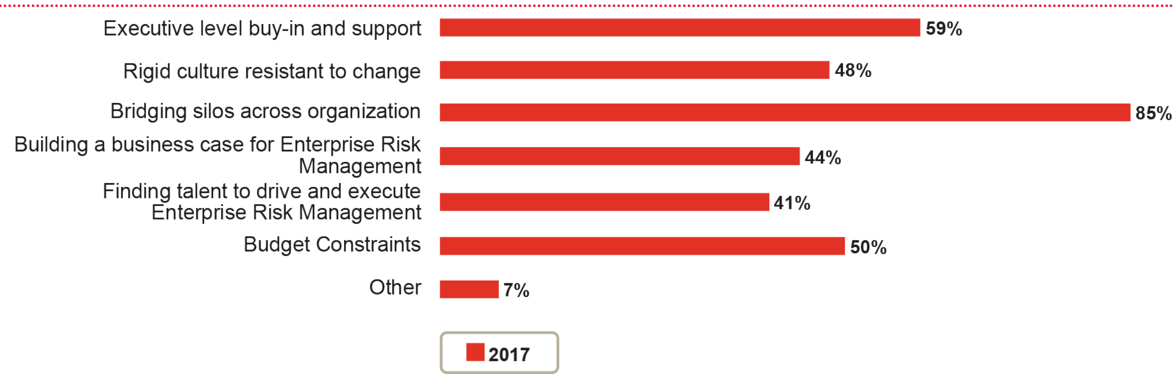


Cultural and leadership constraints continue to dominate the *barriers* associated with establishing an ERM program compared to potential procedural or budgetary limitations. Across all respondents, **85% list "Bridging silos across organization" as the #1 barrier** with "Executive level buy-in and support" coming in second at 59%. These results are fairly consistent across all demographic categories.

In the free response section, conflicting priorities associated with Agency Reform efforts are identified in a few cases as additional barriers in the current Federal environment.

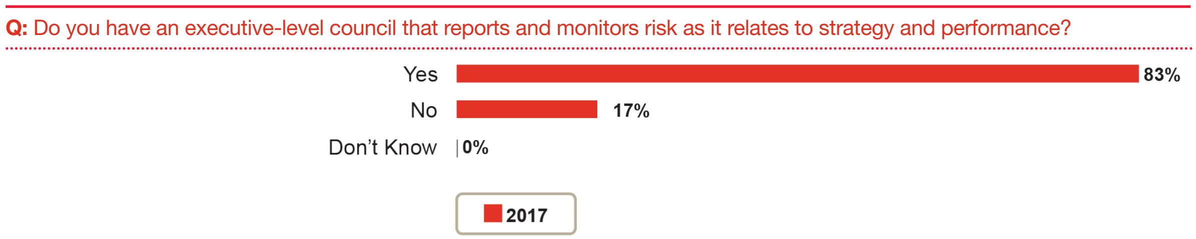
Given the focus of this question on barriers to establishing an ERM program, it is important to focus on the 24% of respondents that work in **organizations that have not yet established a formal ERM program.** For this group, **92% identify both "Bridging silos across organization" and "Building a business case for ERM" followed closely by "Executive level buy-in and support" (85%) as top barriers.** In addition, 69% of these respondents identify "Budget constraints" as a top barrier as well.

Q: Which barriers does your Organization face in establishing a formal Enterprise Risk Management program? Please select all that apply.



Governance & Structure

While some aspects of ERM programs are very consistent across Federal organizations, others vary widely. For example, in one of this year's new questions, **more than 80% of respondents indicate that they have an executive-level council that reports and monitors risk.** The presence of this governance component is comparable (~80%) across all demographic groups, with the notable exception of the longer duration ERM programs from which 100% of respondents report having such a council in place.

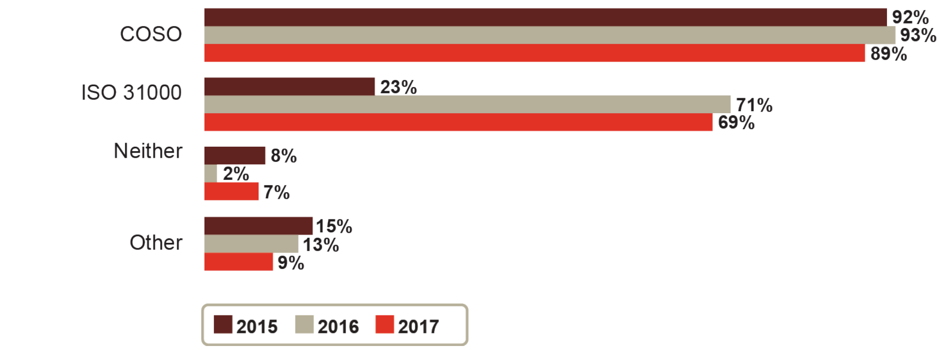


However, **the ERM operating models chosen by Federal organizations vary widely** when considering concepts such as full-time or part-time resources and whether those resources are primarily centralized or decentralized within the organization. The predominate model has full-time resources reporting directly to ERM leadership (41%), but nearly a third of the ERM programs have a more decentralized approach that primarily leverages part-time resources within business units to collect risk-related information to provide to centralized leadership. Organizations led by a CRO and those with longer duration ERM programs are both more likely to have full-time resources reporting directly to the centralized ERM program. However, even within those demographic groups there remains variability with regard to the different kinds of models employed.

Industry Frameworks

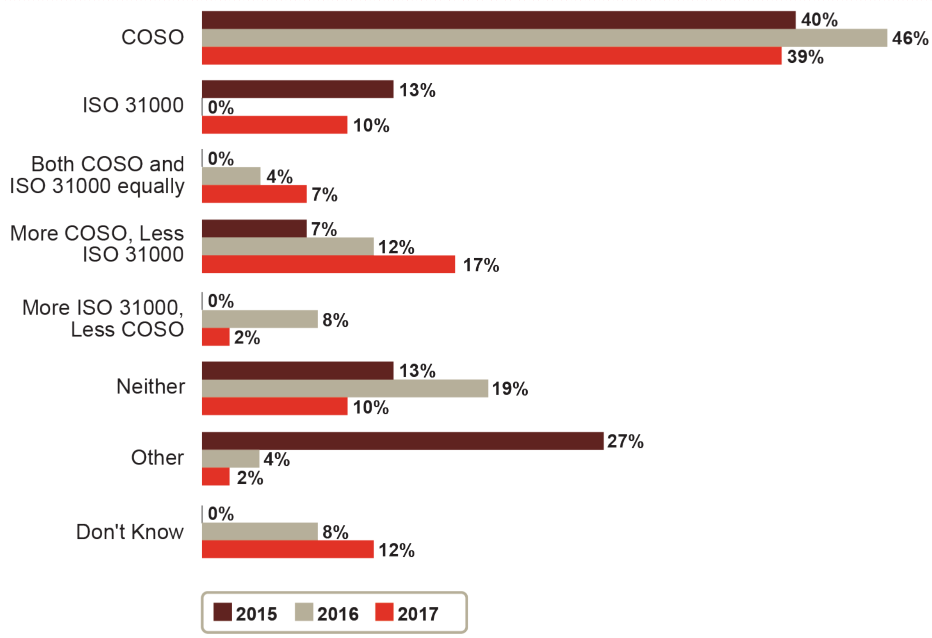
Many aspects of Federal ERM programs are influenced by standards established in ERM frameworks. **For the third straight year, approximately 90% of the respondents to this year's survey indicate that they are aware of the COSO ERM Framework***, with awareness for the ISO 31000 ERM Framework at approximately 70% for the second year in a row.

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



In terms of actual adoption, **COSO continues to be the predominant framework being adopted for Federal ERM.** Nearly 60% of respondents identify either "COSO" or "More COSO, Less ISO 31000" as the predominant industry standard that they follow, compared to 12% for either "ISO 31000" or "More ISO 31000, Less COSO." In terms of demographic breakdowns, COSO is even more pronounced as the dominant standard for ERM for both larger Federal organizations and for those with longer duration ERM programs (ISO 31000 was not selected as the predominant standard for use by anyone in either of these demographic groups).

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

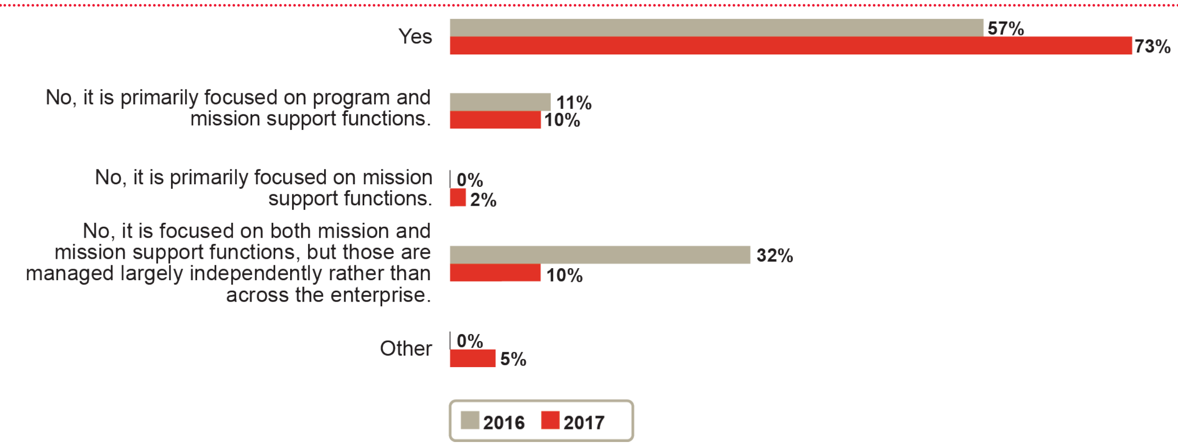


* Editor's Note: PwC was the principal author of the original COSO ERM Framework (2004), and also served as the principal author of the update to the Framework (Enterprise Risk Management: Integrating with Strategy and Performance), which was just published in September 2017.

Program Scope

Nearly three-quarters of Federal ERM programs are focused on a "comprehensive program that encompasses a holistic view of mission and mission support functions" – up from 57% last year. Similar to last year, virtually none is focused primarily on mission support functions. Organizations with comprehensive programs are most prominent in smaller organizations (82%, compared to 54% for larger organizations). In addition, 82% of people working in risk management functions characterize their programs as being comprehensive, compared to 54% for people from non-risk management functions.

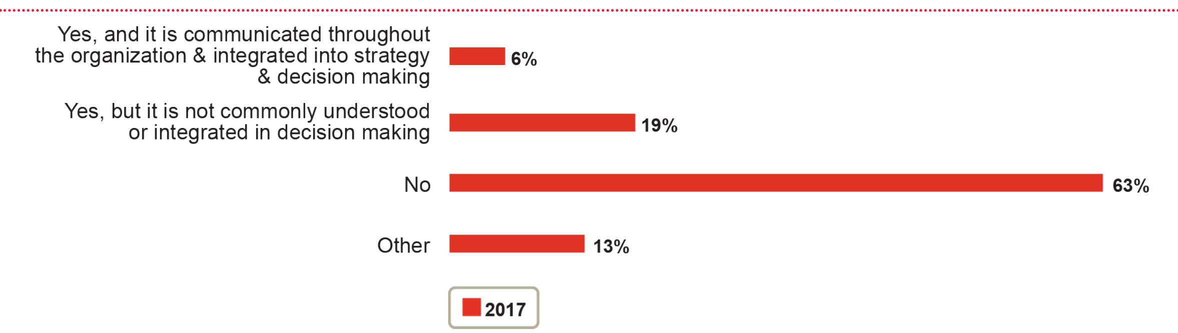
Q: Is the focus of your Organization's ERM program comprehensive, encompassing a holistic view of mission and mission support functions?



The concept of risk appetite can be beneficial to organizations that are trying to gain alignment on how much risk the organization is willing to accept across the enterprise in pursuit of strategic objectives. In a new question this year, survey respondents indicate that the concept of **risk appetite remains in its infancy in its adoption by Federal ERM programs.** Specifically, more than 60% of respondents indicate that their ERM program does not have a defined risk appetite statement, and that number jumps to more than 80% if it includes those organizations that do have a risk appetite statement but it is neither commonly understood nor integrated into decision-making. **Only 6% of respondents indicate that they have a risk appetite statement and that it is both widely communicated and currently integrated into strategy and decision-making.** Similar responses can be found across all demographic groups, including those organizations with longer duration ERM programs. These organizations are more likely to have a risk appetite statement than those with shorter duration ERM programs, but even longer duration programs indicate that their risk appetite statement is not commonly understood or integrated into decision making.

In the free response section for this question, several respondents indicate that their organizations are currently developing risk appetite statements, including organizations that span both shorter and longer duration ERM programs.

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



Integrated Capabilities

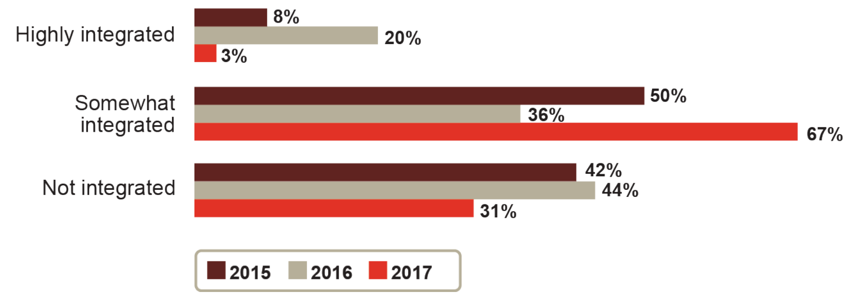
ERM programs often seek to generate value by enhancing leadership decision-making in pursuit of the strategic objectives of the enterprise. As a result, the insights generated by integrating risk into an organization's processes associated with strategic planning, budget, and execution (e.g., performance management and execution oversight) can be useful in seeking to maximize this value proposition. That said, this year's survey indicates that this level of integration is not being achieved by the vast majority of Federal organizations.

Specifically, **only about 5% of respondents indicate that ERM has been "Highly Integrated" with these three business processes** (3% for Strategic Planning, 5% for Budgetary Processes, and 7% for Execution Processes).

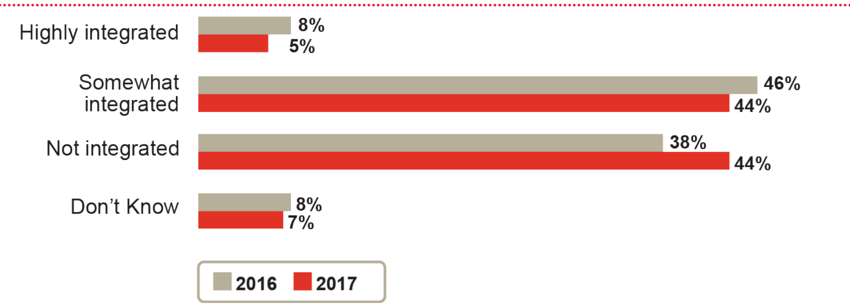
"Somewhat Integrated" is the most common response to these questions (particularly prominent for strategic planning at 67%), but "Not Integrated" is also prominent across the board (between 31% to 44% across the three processes). All of these responses are relatively unchanged from a year ago.*

There is also little deviation in these responses across the demographic groups, including from longer duration ERM programs and from respondents in risk management functions. In both of these cases, the "Somewhat Integrated" response is slightly higher than the "Not Integrated" response compared to organizations with shorter duration ERM programs and those from non-risk management functions. That said, the "Highly Integrated" response remains less than 10% across all these demographic groups.

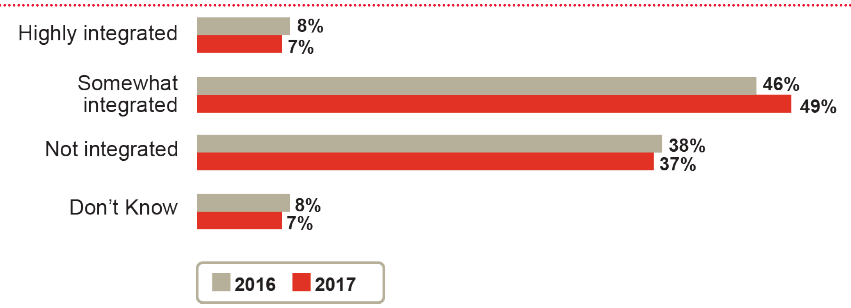
Q: To what extent has your Organization integrated Enterprise Risk Management into strategic planning?



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



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



* Editor's Note: Last year, the integration question related to budgetary processes and execution processes was combined into a single question. For the charts and year-over-year comparison, last year's responses are depicted as the same for this year's separate questions for integration with these processes.

Focus & Priorities

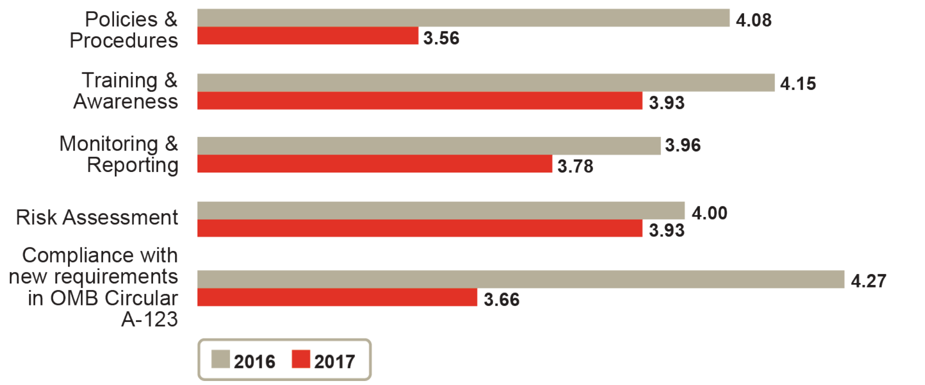
Focus & Improvement Opportunities for ERM Programs for the Next Year

Despite the re-emergence in this year's survey of OMB Circular A-123 as a prominent motivator for the establishment of an agency's ERM program, respondents indicate that **the focus of existing ERM programs over the next 12 months will be much less on A-123 compliance than was depicted a year ago.** Last year, compliance with Circular A-123 was the highest rated focus area, with significant increase in focus anticipated. This year, it is rated #4 out of five, just barely ahead of Policies and Procedures.

Focus on "Training and Awareness" and "Risk Assessment" top the list this year. "Training and Awareness" is particularly prominent as a focus area by longer duration ERM programs and by respondents assigned to risk management functions.

The average score on each of the five topics depicted in this question are lower relative to last year. While this year's scores are still above "No Change," they are less than "Increase Somewhat" on average across the board. This differs from last year when just about all of the responses exceeded "Increase Somewhat," on average.

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.)*



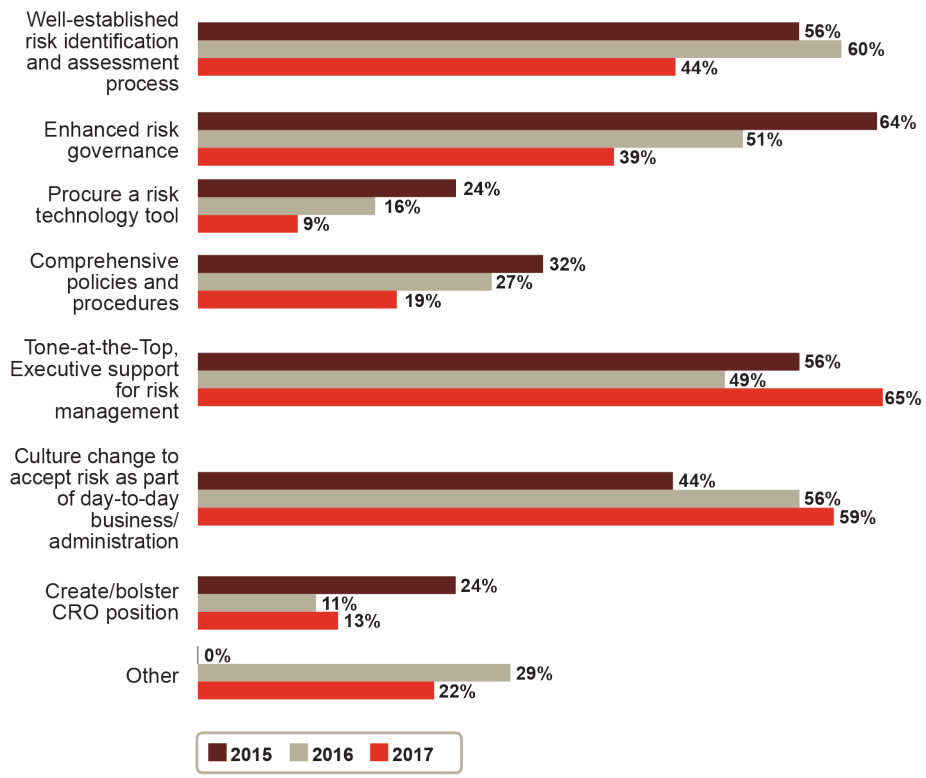
In terms of areas for impactful improvements to position organizations to better respond to risks, "Tone-at-the-Top, Executive support for Risk Management" has the biggest jump, moving from fourth to first in this year's survey. "Culture change to accept risk as part of day-to-day business / administration" is a close second this year, followed by "Well-established risk identification and assessment process" (last year's #1) and "Enhanced risk governance." **Three of these four top areas for impactful improvement emphasize the leadership, culture, and human behavior aspects of ERM far more than the options that focus on processes, procedures, and technology.**

"Tone-at-the-Top" is an especially prominent area for impactful improvement among larger organizations (cited by 83% of respondents) and for those organizations with longer duration ERM programs (71%).

Organizations that do not yet have an ERM program identify "Tone-at-the-Top, Executive support for risk management" as the most prominent means for achieving impactful improvements in managing risks (85%), followed by "Culture change to accept risk as part of day-to-day business / administration" (62%).

"Procuring a risk governance tool" and "Create / bolster CRO position" remain at the bottom of the priority list for impactful improvements for the third straight year.

Q: Please select the most impactful improvements that your Organization could make to be better positioned to respond to CURRENT and ANTICIPATED risks? Please select up to three.



Enterprise Risks

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

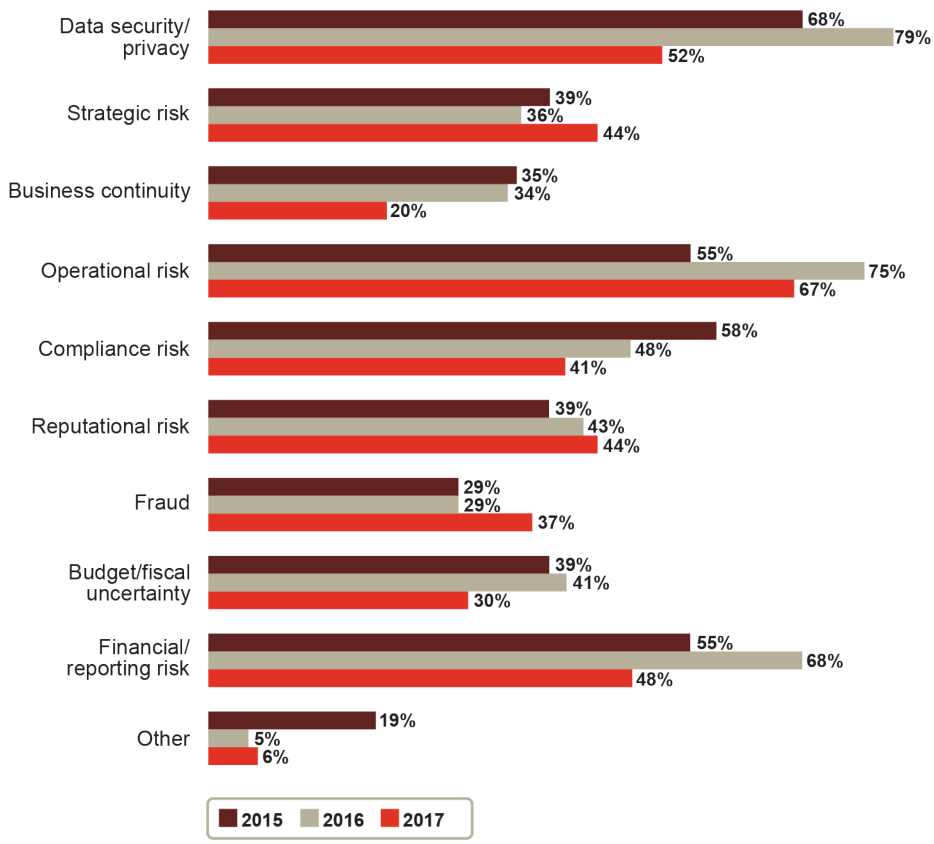
1. Management's current focus on risks
2. Perception of risks currently believed to have the greatest impact on the achievement of strategic objectives, regardless of management's current focus
3. Perception of risks anticipated to have the greatest impact on the achievement of strategic objectives over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

Management's current focus on risks

"Operational risk" moves up a notch to eclipse "Data security / privacy" as the risk area currently receiving the most attention from management, followed closely by "Financial / reporting risk" which remains #3. Strategic and Reputational risk both move up in this category for a tie at #4.

Of note is that respondents from organizations that do not yet have an ERM program place Strategic and Reputational risks at the top of the list receiving focus from management, the only demographic group to do so.

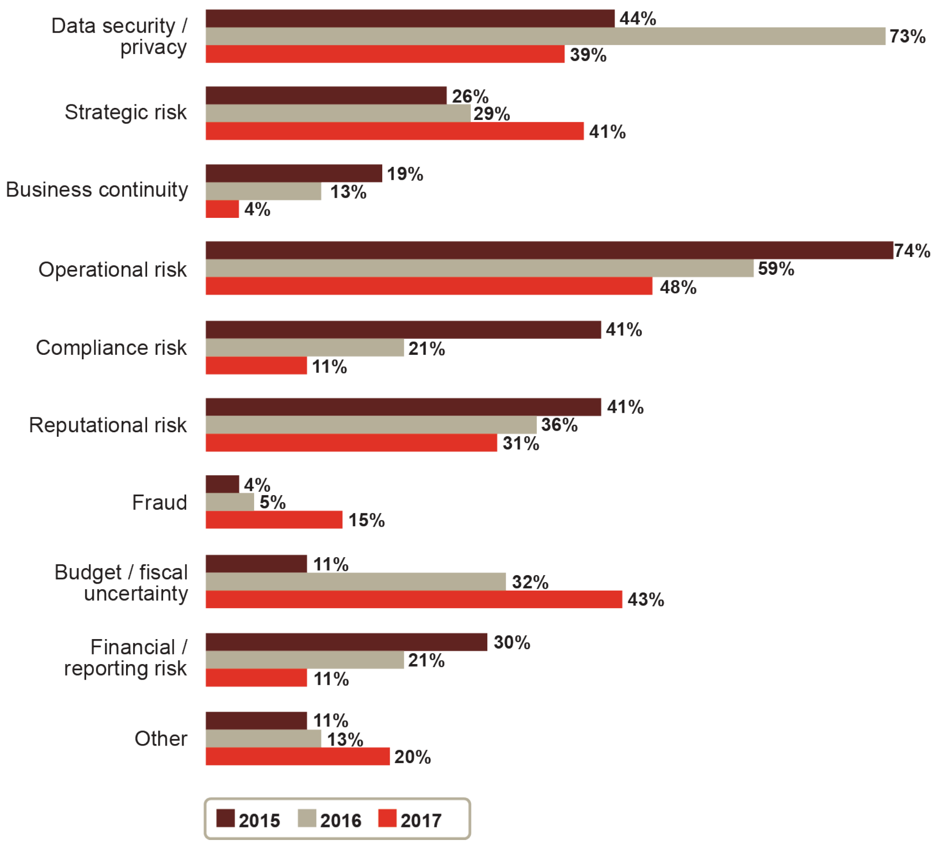
Q: Which types of risk does your management focus resources on the MOST? Please select all that apply.



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

Regardless of management's focus, the perception of current risks and their potential to impact the achievement of strategic objectives is also explored. **"Operational risk" tops the list for both management's current focus and its perception of highest impacting current risks, but the rest of the list introduces some notable changes.** For example, "Budget / fiscal uncertainty" and "Strategic risk" both jumped three spots from a year ago, into the #2 and #3 spots, respectively. After topping the list of current perceived risks one year ago, "Data security / privacy" fell three places to #4 this year with a decline in responses from 73% to 39%.

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.

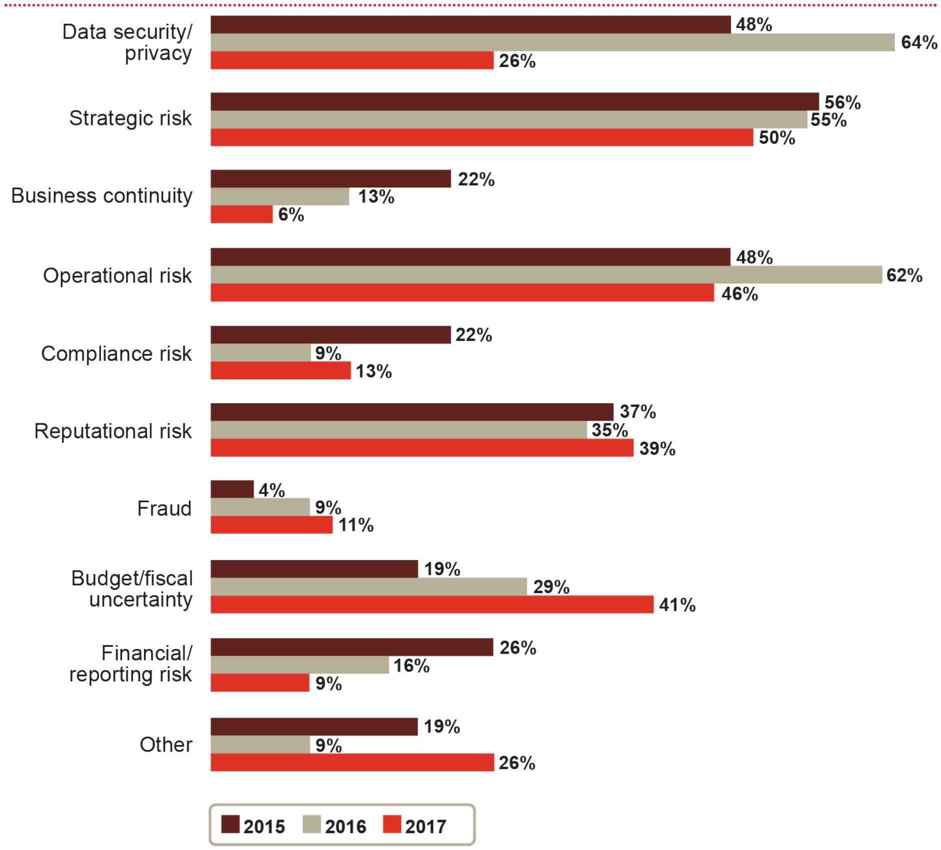


Perception of risks *anticipated* to have the greatest impact on strategic objectives over the next 3-5 years

"Strategic risk" tops this list for the first time in terms of the potential for greatest impact on achieving business objectives over the next 3-5 years, up from the #3 spot a year ago. "Operational risk" retains a high position at #2, followed by "Budget / fiscal uncertainty" which moves up from #5 to #3 this year. Again, "Data security / privacy" falls significantly in this year's responses, dropping from the top spot (64%) to #5 (26% of mentions).

Risks related to human capital are mentioned in approximately 10% of total responses via the free response section provided for these questions.

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 & Future Risks

The previous three questions provide an opportunity to evaluate the degree to which management's application of resources to current risks is aligned with the broader perception of the organization's most significant risks – both in the present and anticipated in the future.

The first observation is that **alignment exists at the top of these lists, as "Operational risk"** is receiving the greatest level of management's current focus, is #1 in perceived current risk, and is #2 in perceived anticipated risk over the next 3-5 years. In addition, there is pretty strong alignment across these three perspectives for both Reputational Risk and Strategic Risk.

However, the rest of the results across these questions demonstrate that a disconnect does exist in a number of key areas.

For example, "Data security / privacy" continues to receive significant management attention (cited by more than 50% of respondents and #2 in this year's survey), but drops off considerably as a perceived current risk (to under 40% of respondents) and drops even further in terms of anticipated future risks (26% of respondents).

Similarly, while "Financial / reporting risk," "Compliance risk," and "Fraud" are all cited by more than 40% of respondents in terms of the types of risk that are currently receiving the most focus by management, all three are rarely cited in terms of actual perception of current or future risk (each around 10%).

One risk type actually goes in the opposite direction: "Budget / fiscal uncertainty," which is cited by 30% of respondents in terms of receiving current management focus, is cited by 43% of respondents in terms of perceived current risk and by 41% for perceived anticipated risk.

Overall, the number of discrepancies cited above represent a lack of strategic alignment for many organizations in terms of their current focus and utilization of resources compared to risk-informed insight as to their greatest current and future risks and their potential impact on the fulfillment of strategic objectives. This finding represents an opportunity to re-visit and perhaps re-prioritize those resource allocations.

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

Execution & Performance

ERM Benefits

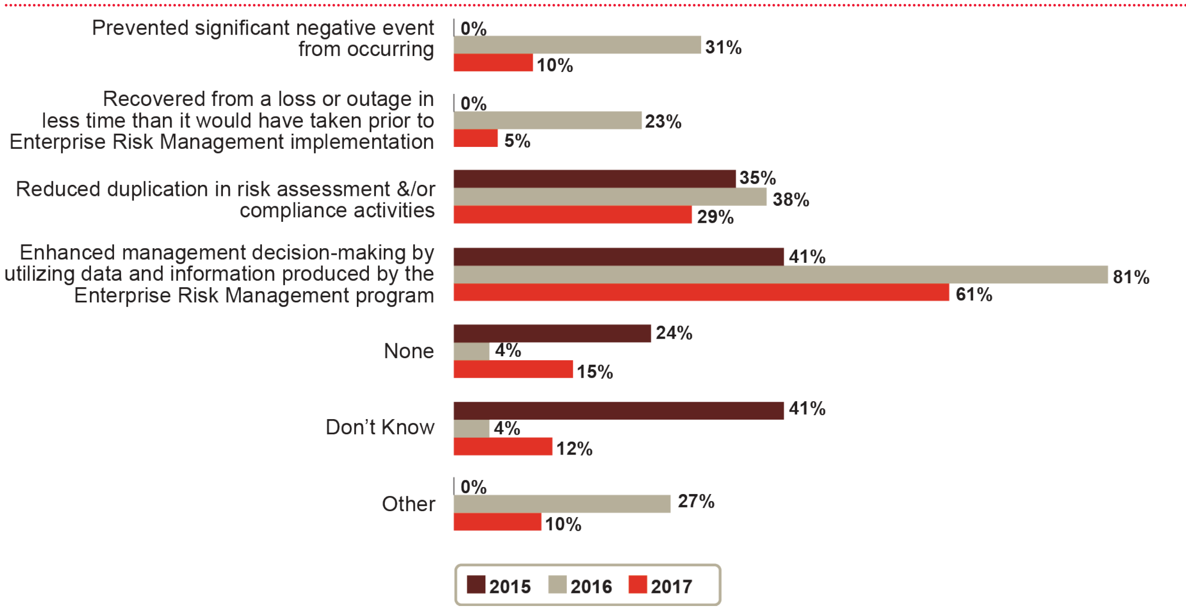
After a surge in reported benefits from the 2015 survey to 2016, **there is a noticeable reduction in identified benefits across most of the listed categories in 2017.** Benefits clearly exist, particularly in the area of "Enhanced decision-making" but the benefits are not as pronounced when compared to last year's survey. **"Enhanced management decision-making by utilizing data and information produced by the ERM program" is still selected as a benefit by 61% of respondents this year**, but that is down from 81% the previous year. Along these same lines, "Prevented significant negative event from occurring" is still cited by 10% of respondents, but that is down from 31% the year before. "Reduced duplication in risk assessment and / or compliance activities" is being experienced by 29% of organizations, down nine points from a year ago.

This downward trend in overall benefits may be impacted by the significant number (46%) of respondents to this year's survey from organizations which have had their ERM program up and running for less than one year. In fact, just under 50% of these new programs indicate that they have realized no benefits in their program in their less than one year in existence. To emphasize this point, several respondents used the free response section to specifically mention that the infancy of their program is a major factor contributing to the lack of benefits realized thus far. "Enhanced decision-making" is the only benefit that is prominent among these new programs.

To further this point, while 15% of the total number of respondents indicate that they have not yet received any benefits from their ERM program, all but one of these responses came from someone whose program has been in existence less than one year. In comparison, longer duration ERM programs (in existence greater than three years) all indicate that they have received some type of benefits from their program.

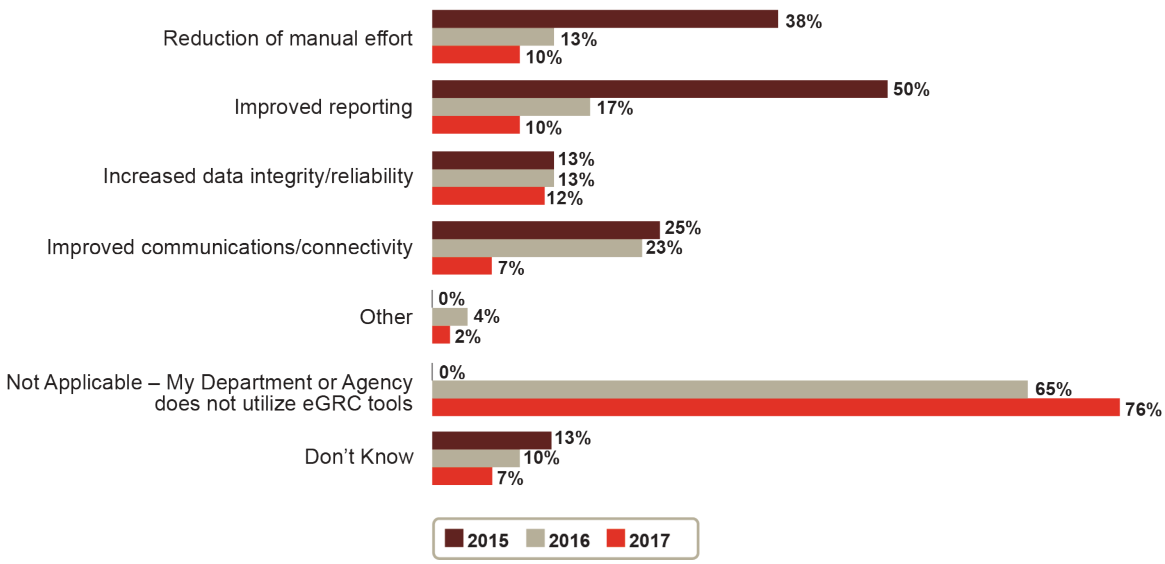
Respondents from **longer duration ERM programs indicate the greatest prominence in the area of benefits, with 86% identifying "Enhanced decision-making" as a result of their ERM program.** Similarly, respondents who work in risk management functions identify "Enhanced decision-making" as a benefit in 71% of responses.

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



Finally, for the third straight year the survey sought to identify benefits being realized by Federal organizations that have implemented an enterprise Governance, Risk, and Compliance (eGRC) tool. While a handful of benefits are identified by a small number of respondents, **three-quarters of respondents indicate that the question is "Not Applicable" since their organization has not implemented such a tool.** That percentage is even higher than the two-thirds who responded similarly last year. Approximately 40% of organizations with the longer duration ERM programs have implemented some form of eGRC tool, with "Increased data integrity / reliability" serving as the greatest benefit. All other demographic categories indicate very low adoption of eGRC tools.

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.

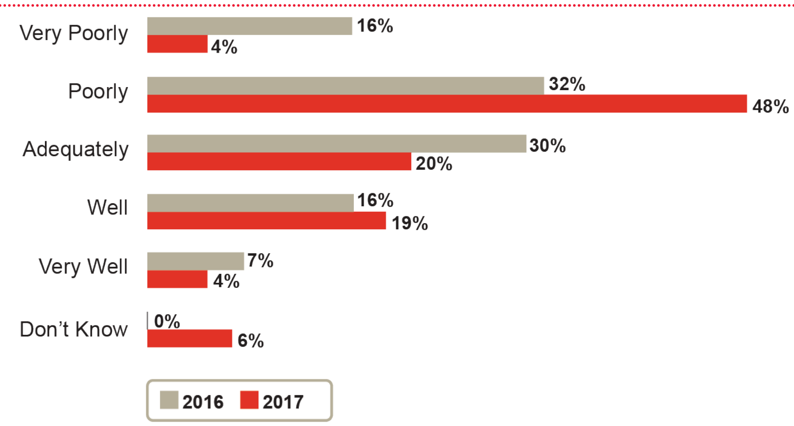


ERM & Culture

Earlier questions and analysis related to ERM and Culture already 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, including the longer duration ERM programs. In this new section of this report, the following responses provide additional insights into the current state of ERM & Culture in the Federal government.

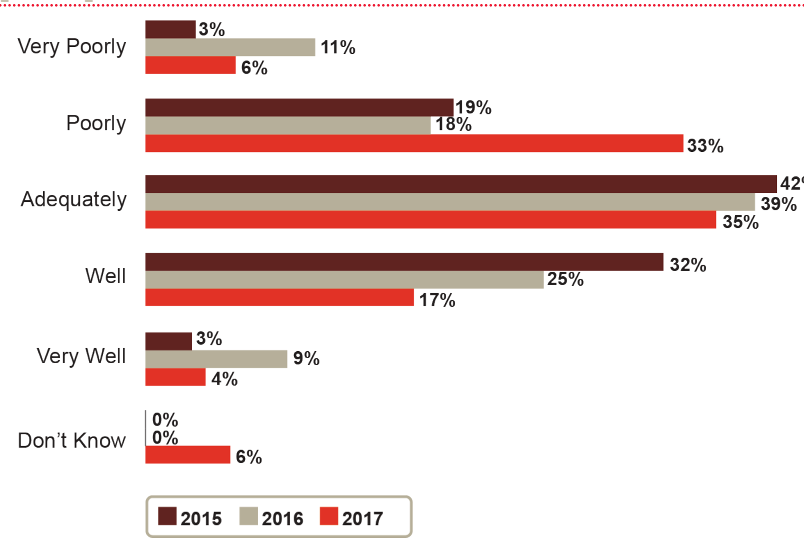
Similar to last year, respondents indicate that **organizations are generally not performing well in embracing the cultural aspects of risk transparency and promoting an environment where managers and staff are open to discussing risks as part of everyday business.** For the second year in a row, "Poorly" and "Very Poorly" combine to top 50% of responses to this question. These results are consistent regardless of the duration of the ERM program or the functional role of the individual respondent. Larger organizations fare worse than the smaller ones, with two-thirds of larger organizations responding "Poorly" or "Very Poorly" compared to 44% for smaller organizations. That said, **organizations without an ERM program struggle even more in this regard with negative responses hitting 70%, compared to 46% for organizations that have implemented an ERM program.**

Q: How do you rate how well your 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?



In terms of **embedding risk management as a component in all critical decisions throughout the organization, the survey indicates a downward shift from a year ago, and a steep drop from the year before** (39% = "Poorly" or "Very Poorly" this year compared to 29% last year and 22% the year before). The "Poorly" and "Very Poorly" percentages increase to 57% for organizations with longer duration ERM programs (30% for organizations with shorter duration ERM programs). In fact, the response profile for organizations with longer duration ERM programs and with no ERM program are considerably worse (both > 50% negative) than those with shorter duration ERM programs. Once again, smaller organizations indicate a much more positive response to this capability when compared to larger organizations.

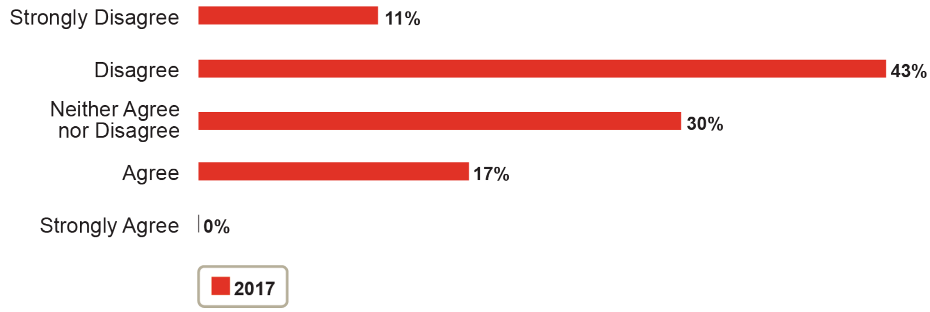
Q: How do you rate how well your Organization seeks to embed risk management as a component in all critical decisions throughout the organization?



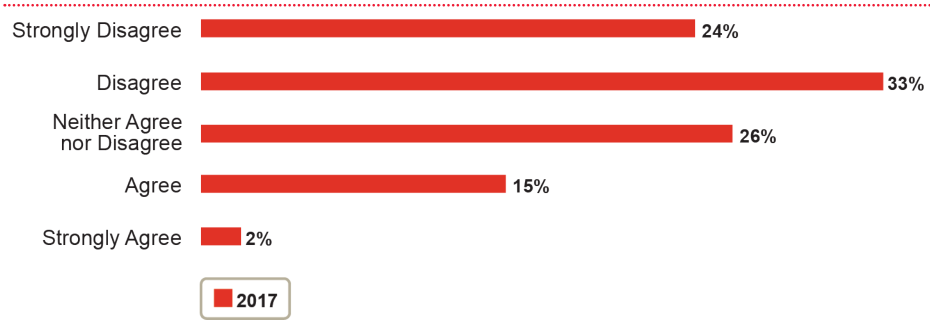
A commitment to training represents another characteristic that can be used to assess the cultural adoption of ERM within an organization. Once again, survey responses indicate that Federal organizations are not faring well in this regard. Specifically, **more than half of this year's respondents indicate that sufficient risk management training is not being provided for staff to effectively carry out their risk management responsibilities.** That compares to 17% who agree with the statement and 0% who strongly agree. This is one area that seems to improve over time as 43% of longer duration ERM programs provide a positive response ("Agree" or "Strongly Agree") compared to 18% for shorter duration ERM programs, and 0% for organizations with no ERM program (the latter listed 77% as "Disagree" or "Strongly Disagree"). People outside of the risk management function are also negative on this topic with 81% selecting "Disagree" or "Strongly Disagree" compared to 36% of individuals from within the risk management function.

Finally, an ERM culture can be evaluated in part by the degree to which the organization's performance management system is aligned to embracing the concept of risk appetite, particularly within contexts where leaders utilize performance management to encourage an appropriate level of risk-taking in pursuit of strategic objectives. **Similar to the previous culture-related questions, 57% of respondents "Disagree" or "Strongly Disagree" with the alignment between an appropriate level of risk-taking with their organization's performance management system**, while 15% agree and 2% strongly agree. This response profile is consistent across all demographic groups, including those from respondents within organizations with longer duration ERM programs and those within risk management functions.

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



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 final section of this year's survey includes responses related to how well people feel their organizations are performing in specific areas related to ERM. In general, responses are similar to those received in the previous year, with most of the results improved over the cultural characteristics previously evaluated, but most remain shifted to the left ("Poorly") on average compared to a traditional "bell curve."

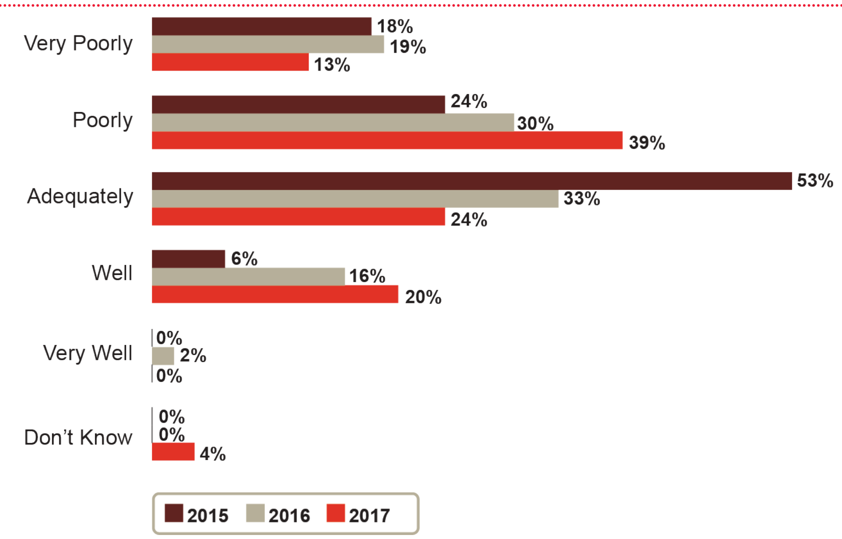
One interesting note that spans the responses across each of these areas is that perceived effectiveness is generally lower for new ERM programs (i.e., in existence less than one year) and for longer duration ERM programs (i.e., in existence greater than three years) when compared to more positive perspectives for organizations that have had their ERM program in the 1-to-3 year range.

In terms of the four risk types identified for managing risk exposure, **Financial Risk has the highest identified level of proficiency, followed in order by Compliance Risk, Operational Risk and Strategic Risk. Strategic Risk has the least level of proficiency across all demographic groups.** Smaller organizations generally report higher scores for proficiency in each risk type when compared with larger organizations.

Prioritizing and managing risk as an interrelated portfolio rather than within individual silos portrays approximately 50% of respondents as "Poorly" or "Very Poorly" for the second year in a row, and none indicating "Very Well." Larger organizations are particularly poor in this area (60% "Poorly" or "Very Poorly"). Having an ERM program, and the duration of that program, also stand out as differentiating characteristics when it comes to this capability. For example, organizations with longer duration ERM programs show improvement in this category when compared to organizations with shorter duration ERM programs, while people from organizations that do not have an ERM program score the lowest overall (70% "Poorly" or "Very Poorly" and 0% "Well" or "Very Well").

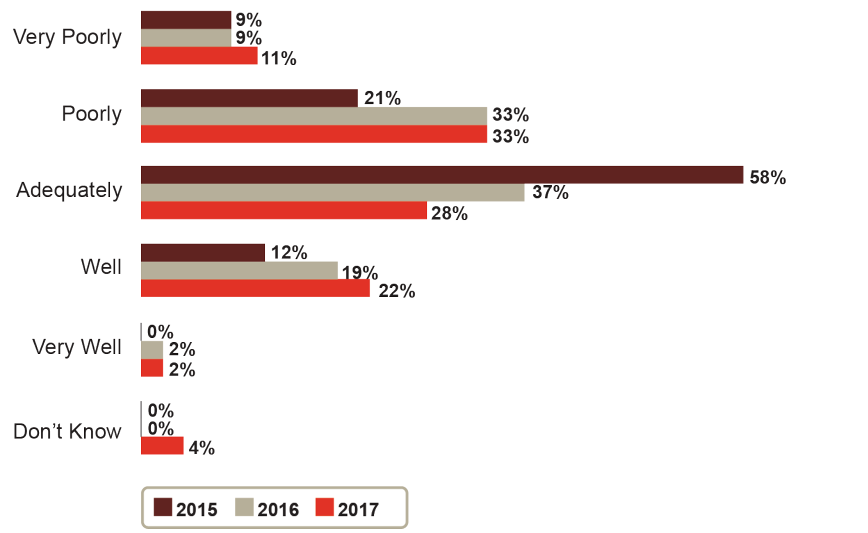
Q: How do you rate how well your Organization manages all areas of risk exposure? *(Results for each risk area are average scores against the following 5-point scale: (1) Very Poorly; (2) Poorly; (3) Adequately; (4) Well; and (5) Very Well.)*

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?



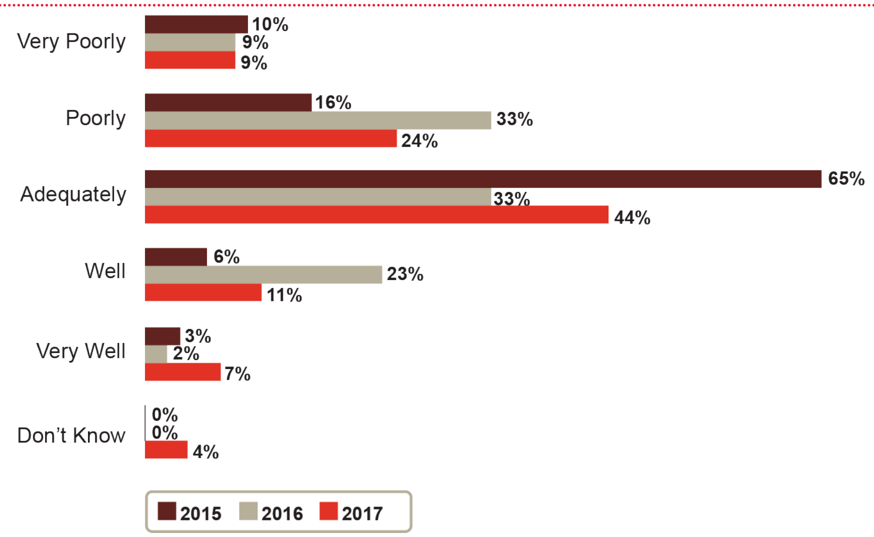
Organizational abilities to evaluate the risk portfolio in the context of all significant internal and external environments, systems, circumstances, and stakeholders, provide results that are also skewed toward the negative with 44% of respondents indicating “Poorly” or “Very Poorly” and only 2% selecting “Very Well.” Organizations with longer duration ERM programs fare slightly better than those with the shorter duration ERM programs, while larger organizations fare the worst with 50% indicating “Poorly” or “Very Poorly.”

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?



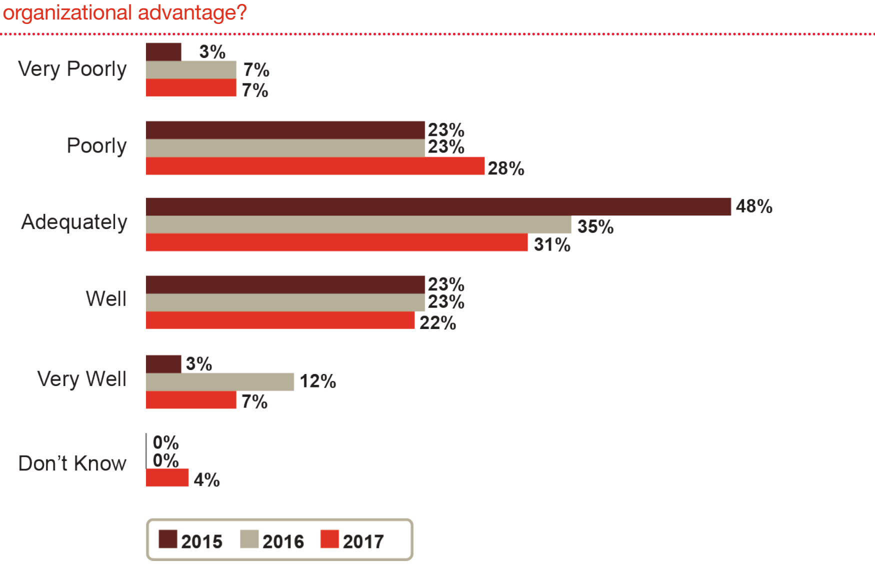
In terms of providing a structured process for the management of all risks, scores improve compared to the previous questions with the response profile being closer to a balanced “bell curve” and a mean result centered on the middle response choice (“Adequately”). The strongest responses are from organizations with the longer duration ERM programs and from people working in a risk management function.

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



How well an organization views the effective management of risk as a value add / organizational advantage also provides results that closely approximate a balanced “bell curve” even though the average scores are still slightly below “Adequately.” Once again, smaller organizations have slightly better results than larger organizations. Organizations without an ERM program have the lowest results with slightly more than half of the respondents selecting “Poorly” or “Very Poorly.”

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



About Us

PwC

PwC helps organizations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 195,000 people who are committed to delivering quality in assurance, tax and advisory services. Find out more and tell us what matters to you by visiting pwc.com/publicsector.

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, PwC's Public Sector 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 PwC Public Sector'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.

Malcolm Baldrige
National Quality Award
2014 Award Recipient

Acknowledgments

This survey report is the product of a collaborative effort between PwC 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

PwC

pwc.com/publicsector

David Fisher
fisher.m.david@us.pwc.com

Cameron Arimoto
cameron.arimoto@us.pwc.com

Rosa Milani
rosa.milani@us.pwc.com

AFERM

www.AFERM.org

Sallyanne Harper
saharper1@verizon.net

Peggy Sherry
president@aferm.org

Todd Grams
tgrams@deloitte.com

Additional contributions from: Tony Elachkar, Kate Sylvis, Meris Yee, Kathleen Zelnik, Thomas Holland, Regina Castaneda, George Park, Brandon Leavitt, Claire Raskob, and Brian Howell.

Creative: *Lauren Gormley*

Contacts

For more information, please contact:

David Fisher
Managing Director
Public Sector Risk Consulting Leader
fisher.m.david@us.pwc.com
(703) 610-7505

Peggy Sherry
President-Elect
Association for Federal Enterprise Risk Management
president@aferm.org

pwc

AFERM
Association for Federal Enterprise Risk Management

www.pwc.com/publicsector

Follow us on Twitter
@pwc_usgov