KPMG

Your risk culture: An ERM enabler or barrier?

AFERM
Association for Federal
Enterprise Risk Management

October 2018

KPMG Government Institute
kpmg.com/us/governmentinstitute

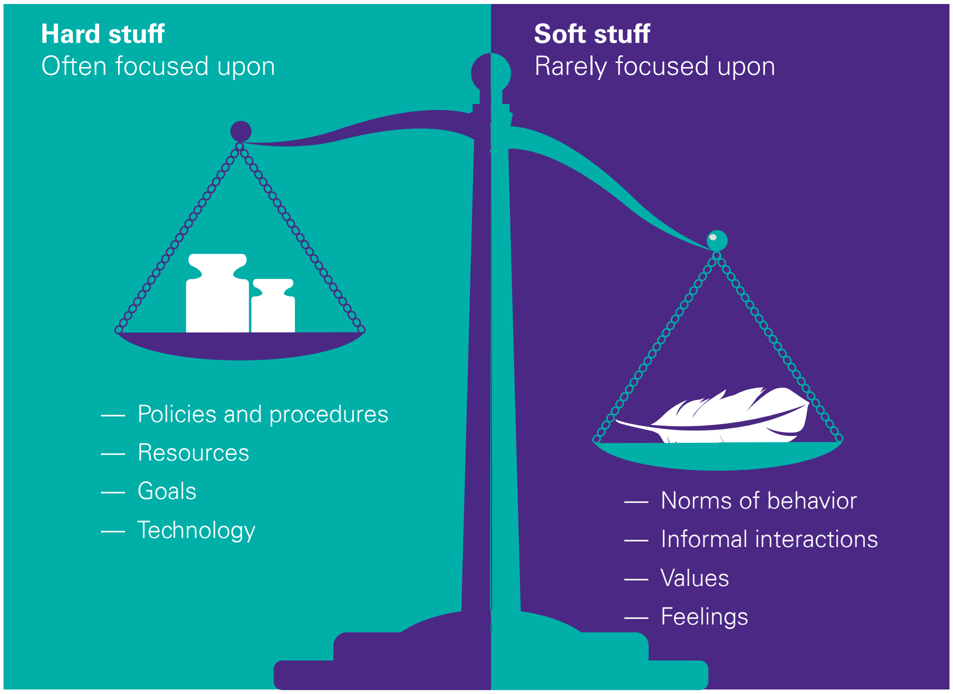
Contents

Introduction

On July 15, 2016, the Office of Management and Budget (OMB) issued the most significant revision to Circular A-123 in over 30 years, mandating that federal agencies adopt enterprise risk management (ERM).[1] Implementation will require significant operational changes. Even more so, success will hinge on agencies' abilities to transform their norms, attitudes, and behaviors relative to risk management, meaning their risk culture.

You may be thinking, why the focus on culture? Isn't that the "soft stuff" on the management continuum? Instead, just tell us how to implement OMB's new technical requirements. Well, culture is the "soft but hard stuff" that is too often overlooked. While it may be rarely focused on, its weight is undeniable as it drives what actually happens in organizations and how individuals personally react to change in their everyday lives. As depicted in Figure 1, the soft stuff carries considerable weight in what is valued and what happens in organizations. An organization's culture exists whether its leadership intentionally seeks to cultivate one or not.

Figure 1: Organizational culture can tip the scales



[1] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-17.pdf.

Mahatma Gandhi said, "A nation's culture resides in the hearts and in the soul of its people." Risk culture—the human factor—truly is the heart and soul of ERM. Moreover, culture is something that must be actively cultivated in order to achieve the desired result. The question is not whether or not an organization has a culture, but rather is that culture aligned with the organization's mission, vision, strategy, and values.

A strong risk culture starts with clear and intentional ownership and commitment by top management that permeates throughout the organization. Everyone needs to clearly understand their role and responsibility for risk management in the context of the organization's mission, vision, strategy, and core values, as well as their assigned job responsibilities. Risk management should be understood as an integral part of day-to-day program and operational management. Moving to ERM is especially challenging when the following conditions are present:

— Deeply entrenched norms, attitudes, and beliefs that are not open or transparent and/or are inconsistent with the organization's mission, vision, strategy, and/or core values.

— Rewards and incentives that encourage bad behavior and discourage behavior that is aligned with desired outcomes.

— Organizational silos or even silos within silos (i.e., "micro-cultures") that are largely insular and lacking mechanisms for collaboration and/or communication across boundaries.

— Natural fear of and even strong resistance to change.

— Staff concerns about retaliation or not being seen as a team player when they communicate information about risks, problems, concerns, or new ideas.

— A prevailing view, often from the top, that culture is the "soft stuff", and thus unimportant and too hard to measure and understand.

As OMB stated in its memorandum to the heads of executive departments and agencies transmitting the revised Circular A-123, renamed Management's Responsibility for Enterprise Risk Management and Internal Control: "Successful implementation of this Circular requires Agencies to establish and foster an open, transparent culture that encourages people to communicate information about potential risks and other concerns with their superiors without fear of retaliation or blame. An open and transparent culture will result in the earlier identification of risk, allowing the opportunity to develop a collaborative response, ultimately leading to a more resilient government."

This white paper, developed by the KPMG Government Institute[2] in collaboration with the Association for Federal Enterprise Risk Management (AFERM), explores risk culture in the context of four fundamental questions.

1 Why focus on risk culture?

2 What are the fundamental considerations in changing the risk culture?

3 What are the attributes of leading risk cultures in government?

4 How do organizations address gaps in their risk culture?

The white paper incorporates results from the 2017 Federal Enterprise Risk Management Survey, performed by PwC in collaboration with AFERM (2017 ERM Survey).[3] This third annual survey included additional targeted risk culture questions to support development of this white paper. Survey respondents saw culture as really mattering. They identified cultural and related constraints as the dominant barriers to implementing ERM.

[2] Also see related thought leadership, "It's Time to Seize Opportunity," AFERM Updates, Issue 20, December 2016; and "Navigating Uncertainty through ERM – A practical approach to implementing OMB Circular A-123," KPMG Government Institute, November 2016.

[3] https://www.aferm.org/wp-content/uploads/2017/11/pwc-public-sector-2017-federal-erm-survey.pdf.

Why focus on risk culture?

The answer is simple: It drives how people think and what they do. View culture as the compass for all behaviors within a government agency. It is an organization's True North Star and the default setting for norms, attitudes, and behaviors that members of the organization will demonstrate. Culture operates in the absence of formal direction, such as written policies and procedures, and influences what actually happens even when there is formal direction. If an organization does not actively and intentionally cultivate a strong risk culture, the benefits of ERM will not be fully realized, and the likelihood of veering off course from an agency's desired goals and outcomes increases.

Risk culture is a vital component of ERM

Figure 2 depicts the relationship of the risk culture to a broader organizational framework for ERM.

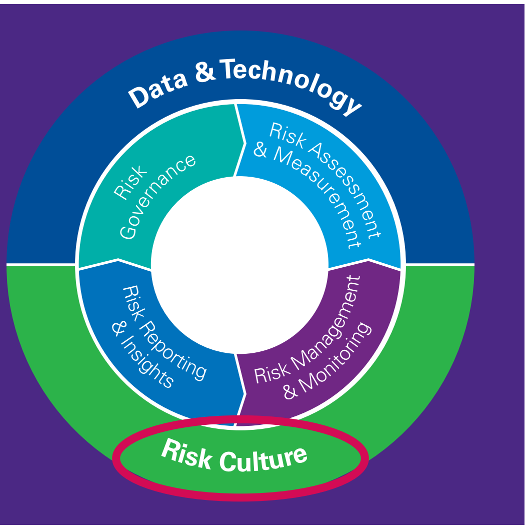
Figure 2: Risk culture is an integral part of ERM

Risk culture is one of the key elements in an organization's Enterprise Risk Management Framework.

Risk culture both influences and is influenced by the other ERM framework elements.

Risk culture influences an organization's risk appetite and governance in a reciprocal manner.

Recent research demonstrates that it is possible for an organization to evaluate their risk culture specifically and to measure the system of values and behaviors present throughout an organization that shape risk decisions.


Data & Technology
Risk Governance
Risk Assessment & Measurement
Risk Reporting & Insights
Risk Management & Monitoring
Risk Culture

Whether in government or the private sector, culture is viewed as one of the most important drivers of favorable results. A 2016 survey of executives from more than 1,300 North American firms revealed that, while executives realized the importance of culture, very few leaders believed they actually had the kind of culture their organizations needed.[4] Here are some of the survey findings regarding the importance of corporate culture:

- 91 percent of executives believed culture is "important" or "very important" at their firm.
- 79 percent ranked culture as at least a "top 5" factor among all things that make their firm valuable.
- 92 percent responded that improving the culture would increase firm value.
- 85 percent believed a poorly implemented, ineffective culture increases the chance that an employee might act unethically or even illegally.
- Only 16 percent said that their firm's culture is where it should be.
- Key cultural values cited by respondents included integrity, collaboration, and adaptability.

[4] Corporate Culture: Evidence From the Field," by John R. Graham, Duke University and the National Bureau of Economic Research (NBER), Campbell R. Harvey, Duke University and NBER, Jillian Popadak Grennan, Duke University, and Shivaram Rajgopal, Columbia University, posted July 9, 2016 and last revised June 4, 2018.

Culture drives behavior

All organizations have a culture, even if it is not formally documented or actively cultivated. The real question is whether the culture is aligned with the organization's mission, vision, strategy, and values. Leading organizations strive for a culture that not only promotes and incentivizes results, but is sensitive to how such results are achieved. The COSO ERM Framework, which is cited in OMB Circular A-123, states that culture "… determines what actually happens, and what rules are obeyed, bent, or ignored."[5]

From the International Institute of Finance, Reform in the financial service industry: Strengthening Practices for a More Stable Systems (2009), an organization's risk culture represents. "The norms of behavior for individuals and groups within an organization that determine the collective ability to identify and understand, openly discuss and act on the organization's current and future risk."

Culture comes in many forms—all impacting how people think and operate as well as representing what they value. Some aspects are supportive of change, while others, such as fear of the unknown, may be resistant. Culture may be observed in written policies or through casual conversations. When you hear someone say: "but we've always done it this way, and it works fine" or "it won't work here," they are describing an organizational culture that embraces the status quo and may not be open to change. That is why having a focus on culture is paramount to successfully implementing ERM. The cultural focus must come from top leadership and be widely understood and embraced throughout the organization. There has to be strong trust in leadership, and leaders have to "walk the talk."

When one looks at major catastrophes and missed opportunities, whether in government or the private sector, organizational culture emerges as a root cause. The culture may have been:

— Largely reactive and not at all well prepared for the worst-case scenario

— Overly insular, with limited desire to adapt and to work across boundaries, and a strong desire to perpetuate the status quo

— Inattentive to significant changes in the environment, such as the opportunities and perils of a cyber world

— Focused on perverse rewards and incentives that encouraged excessive risk taking and are overly - focused on "winning" without regard for how such results are achieved.

[5] COSO (Committee of Sponsoring Organizations of the Treadway Committee) Enterprise Risk Management – Integrating with Strategy and Performance, June 2017.

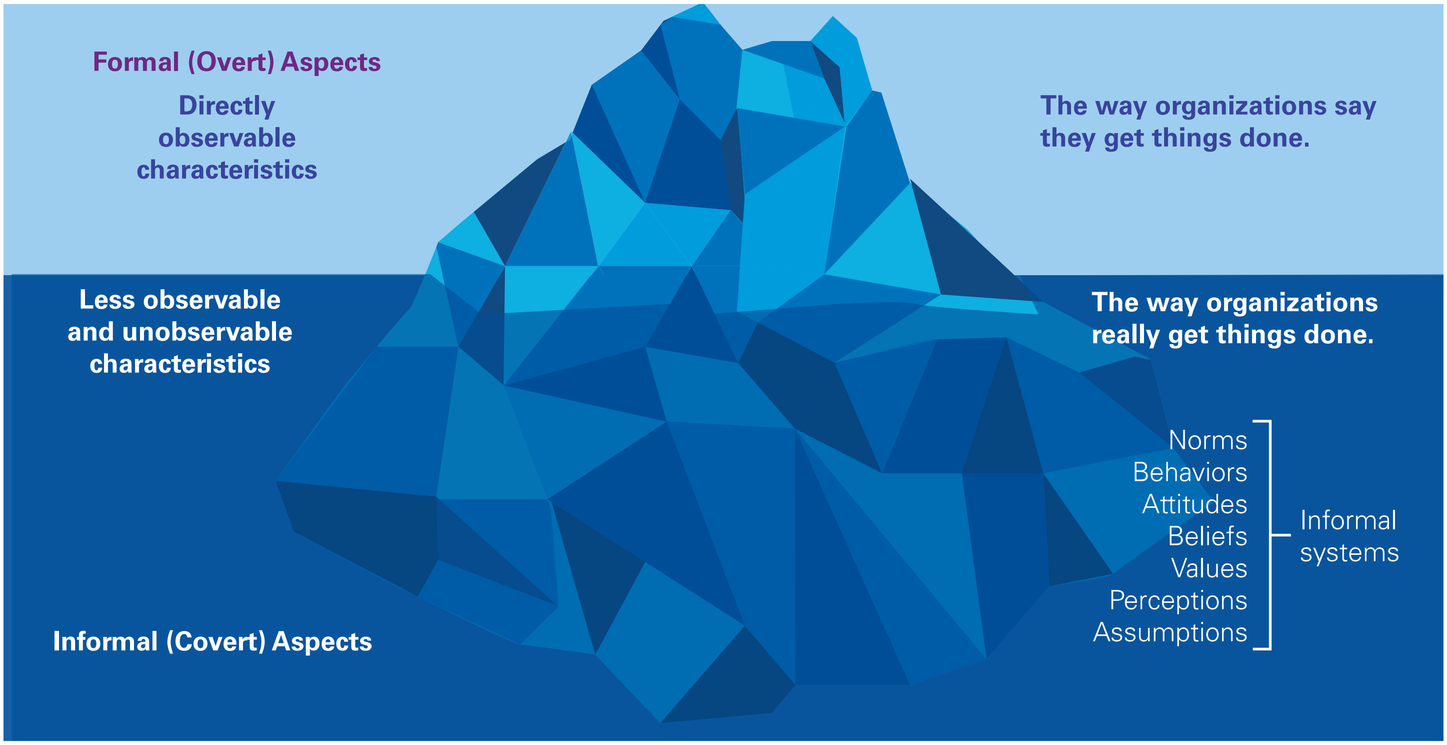
Culture runs deep below the surface

An organization’s risk culture reflects the collective norms, values, attitudes, and behaviors of members of the organization. This is true whether the organization is newly formed or is a more established institution that has been built over decades as is the case for most federal agencies. Reshaping or changing the risk culture takes time and considerable effort as it involves increasing both individual and collective awareness and changing sometimes deeply-rooted behavior and biases as to how things should be done.

A good analogy for culture is an iceberg, since they move slowly and the largest part is below the surface and largely unseen. Similarly, the most important aspects of culture are those that exist unseen beneath the surface. Above the surface are those formal aspects affecting culture, such as policies, procedures, published core values, and ethics and compliance training. These aspects describe how the organization “says” things are supposed to work. There are attributes above the surface that can be readily seen, such as a dress code or a rigidly hierarchical organization structure. But what happens below the surface drives how things “really” work and what gets done.

As shown in Figure 3, like as iceberg, think of culture as having distinct layers, which are hardened and go deep below the surface, and for which change moves slowly.

Figure 3: Risk culture is multi-layered


Formal (Overt) Aspects
Directly observable characteristics
The way organizations say they get things done.
Less observable and unobservable characteristics
The way organizations really get things done.
Norms
Behaviors
Attitudes
Beliefs
Values
Perceptions
Assumptions
Informal systems
Informal (Covert) Aspects

Observable characteristics are above the surface. They are what outsiders can most easily see and may view as the culture. As stated earlier, an example would be published formal core values. But observable characteristics only tell a small part of the culture story.

Norms, behaviors, and attitudes form the top layer below the surface. They may not be seen or seen clearly from outside the organization, but are well known and understood inside the organization and can run deeply below the surface.

Beliefs, values, perceptions, and assumptions represent the deepest layer. They are only seen and understood within the organization and are the most difficult to change. In the federal government where political leadership turns over frequently, these can be difficult to readily discern by new leaders, who may only serve in the position for one to two years.

Each layer will have to be addressed in moving the bar toward a culture that embeds sound risk management concepts in the day-to-day organizational fiber and drives how people think and act in managing risk.

2017 ERM Survey results point to culture as the top barrier to implementing ERM

The 2017 ERM Survey respondents have spoken: "Cultural and leadership constraints continue to dominate the barriers associated with establishing an ERM program compared to potential procedural or budgetary limitations."[6] They can be an absolute show stoppers for meaningful adoption of ERM concepts. Culture and the leadership that is essential to establishing the proper risk culture, drive how the organization operates. They represent what an organization values and how it carries out its mission.

Survey respondents identified six principal barriers, all impacted by the culture

1. **Bridging silos across the organization:** Cited by 85 percent of the respondents, silos touch all three layers of an organizational culture and tend to go very deep. There may be cultures within cultures, whereby organizations within an agency operate independently of each other and have entirely different cultures. Think of organizations in large federal agencies with related missions that find it difficult to work together.

   ERM represents an enterprise look at risk. Operating as independent silos can greatly limit the ability to identify and address risks across an agency. On their own, silos can represent enterprise risks that negatively impact mission effectiveness and efficiency. The President's Management Agenda states that "Silos across Federal agencies and offices can hurt cross-agency collaboration, resulting in fragmented citizen services or excessive cost to deliver the mission."[7]

2. **Executive level buy-in and support:** Cited by 59 percent, top leadership is critical to the culture of any organization, and a strong tone at the top is absolutely essential to the success of any change initiative. This is usually highly observable and above the surface. At the same time, what happens below the surface can negate a leader's desire for change and, in some cases, may even raise questions about the degree to which top management is really committed to change.

3. **Budget constraints:** Cited by 50 percent, not seeking, receiving, and/or allocating adequate funding can result from cultural indifference by top leadership to the importance of ERM.

4. **A rigid culture resistant to change,** was cited by 48 percent of respondents. It touches all three layers of culture and may be even more difficult to address than silos. Time and time again, strong resistance to change has been a showstopper. In government, where top political leadership can frequently turn over, the culture may be one of avoiding change by slow rolling the leader.

5. **Building a business case for ERM,** at 44 percent, can be adversely impacted by the culture. Organizations may have had difficulty seeing the value of ERM and making the best effort to negotiate the rigors of changing the status quo.

6. **Finding the talent to drive and execute ERM** was cited by 41 percent. Again, there may not have been a high enough priority placed on identifying the needed talent or even determining what skills are needed. This can stem from a lack of top management support and a culture that is not supportive of ERM.

[6] See footnote 3.
[7] "President's Management Agenda," March 20, 2018 (https://www.whitehouse.gov/omb/management/pma/).

One in four responded that their organization had not yet established an ERM program

At the time of the 2017 ERM Survey, the requirement for ERM had been in effect for over a year. Also, the changes to OMB Circular A-123 were vetted for several years before the revised Circular was finalized, and in 2015 a new section on the value of ERM was added to OMB Circular A-11, Preparation, Execution, and Submission of the Budget. So, agencies were made well aware that change was coming.

For those respondents who said there organizations had not established ERM programs:

- — The top barriers at 92 percent were bridging silos across the organization and building a business case for ERM.
- — 85 percent cited executive level buy-in and support.
- — 69 percent cited budget constraints, which again could be the result of cultural indifference or an unrealistic expectation that more funding will follow any required change to the status quo.

Respondents also point to the relative infancy of established ERM programs and the risk cultures that serve as the foundation.

For example, the survey found that:

- — Many ERM programs continue to be relatively small initiatives, especially in the context of the over $4 trillion spent by the federal government annually. Twenty percent of the survey respondents reported that their organizations spent $25,000 or less implementing ERM, with another 27 percent reporting that their organizations spent between $25,000 and $250,000. Another 24 percent did not know how much was being spent on ERM.
- — Only 6 percent responded that their organization had a defined risk appetite that had been communicated throughout the organization and integrated into strategy and decision - making. Another 19 percent responded that, while they had a risk appetite, it had not been communicated or integrated.
- — Only 5 percent responded that ERM was highly - integrated into the budgetary process, and only 7 percent said it was highly integrated into the budget execution process.
- — 80 percent believed that ERM activities would increase over the next three years. This was slightly tempered by the 11 percent that saw a decrease and the fact that the baseline of activities reported above was limited.
- — 73 percent responded that their ERM programs were comprehensive, meaning they encompassed "a holistic view of mission and mission support activities," which is what OMB Circular A-123 expects. But given the limited investment, it does not necessarily mean that these programs were by any measure robust at this stage.

To embed ERM in day-to-day operations and decision making, and thereby achieve the results possible, requires a quantum shift in how the requirements in OMB Circular A-123 are viewed. Leading organizations will focus from the outset on building an ERM program that is transformational and reaches deeply into the programs and daily operations.

Tone at the top and cultural change to accept risk were seen as the most impactful improvements organizations could make

The 2017 ERM Survey identified "Tone at the Top, Executive support for risk management" and "Cultural 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." This further drives home the vital importance of culture in driving ERM.

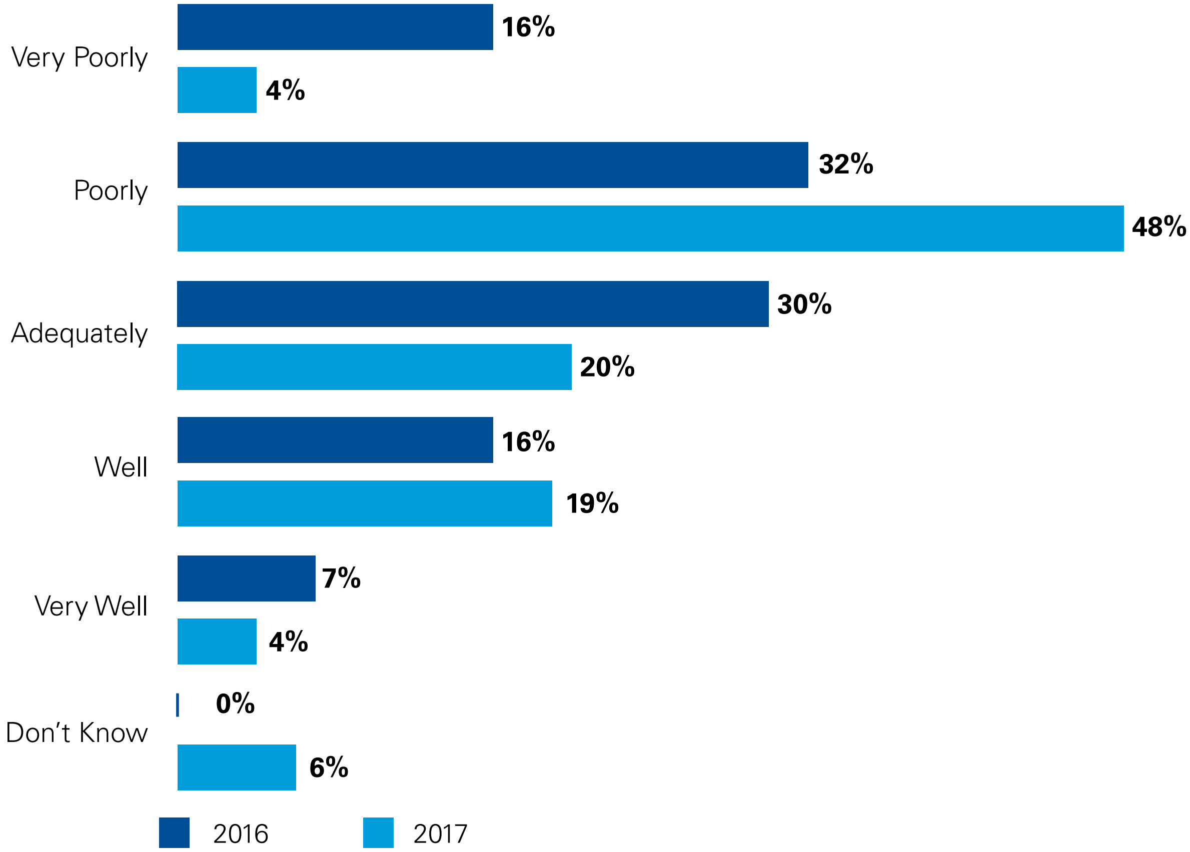
Four other survey questions point to culture as the largest barrier

AFERM Survey respondents were asked the question: "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 part of everyday business?"

As shown in Figure 4, for the second year in a row, over 50 percent of the respondents answered poorly or very poorly. It is markedly worse for larger organizations where two-thirds of respondents have this belief versus 42 percent of respondents from smaller organizations. In either case, this represents a serious barrier to ERM implementation. Just as telling, only 23 percent answered well or very well.

Figure 4: Survey question

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?

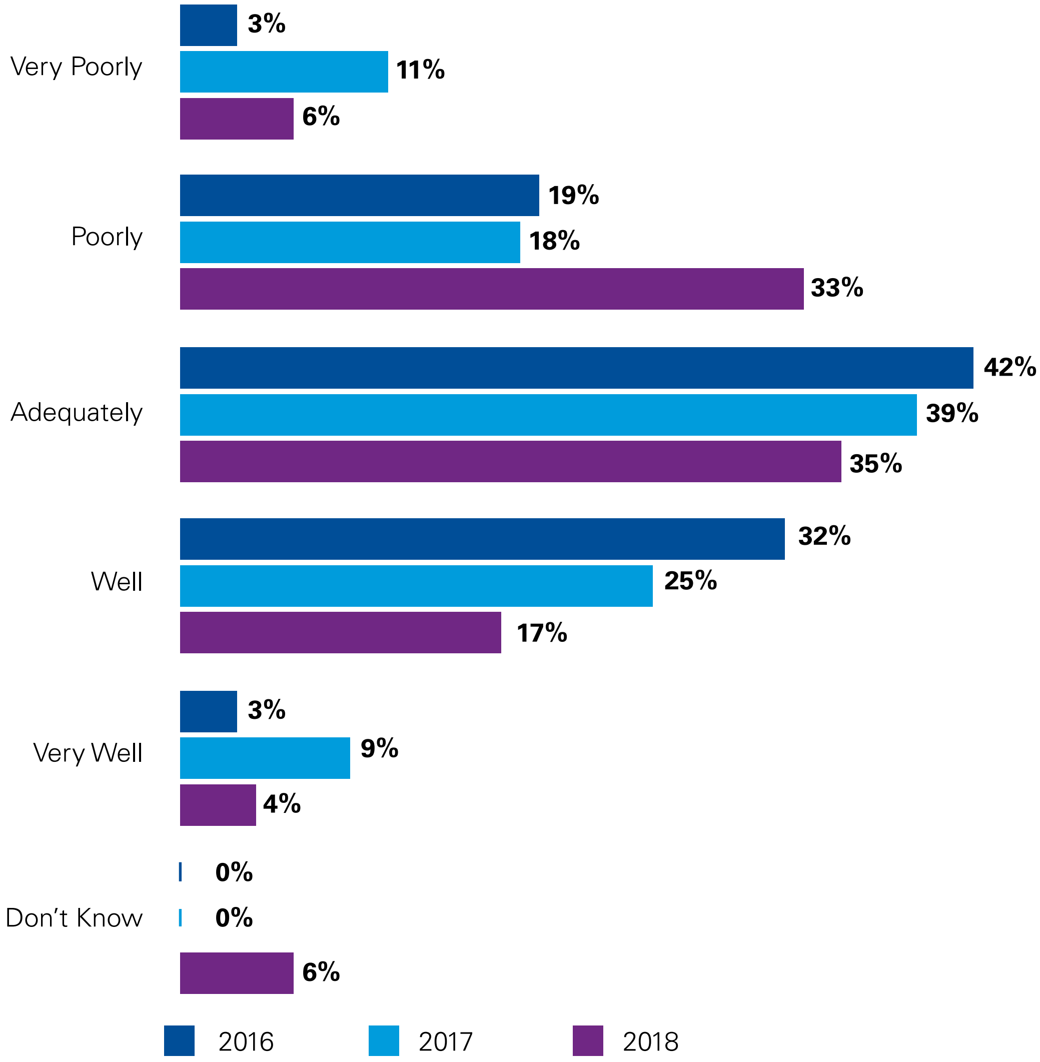


Source: 2017 Federal Enterprise Risk Management Survey, PwC and AFERM.

Finally, three other survey questions point to challenges in adopting an ERM culture, as shown in Figures 5 to 7 below. With respect to all three questions, the percentages of respondents answering well/very well or agree/strongly agree were 21, 17, and 15 percent respectively; whereas, poorly/very poorly and disagree/strongly disagree were at 39, 54, and 57 percent respectively.

Figure 5: Survey question

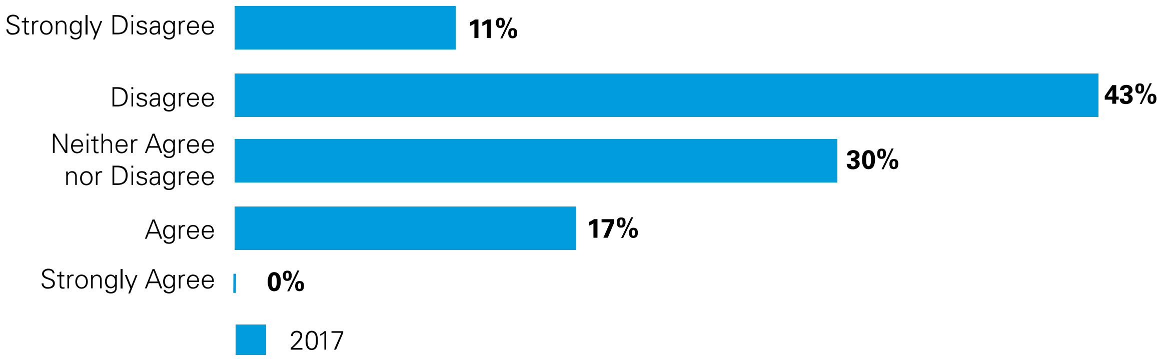
Q: How do you rate how well your Organization seeks to embed risk management as a component in all critical decisions throughout the organization?



Source: 2017 Federal Enterprise Risk Management Survey, PwC and AFERM.

Figure 6: Survey question

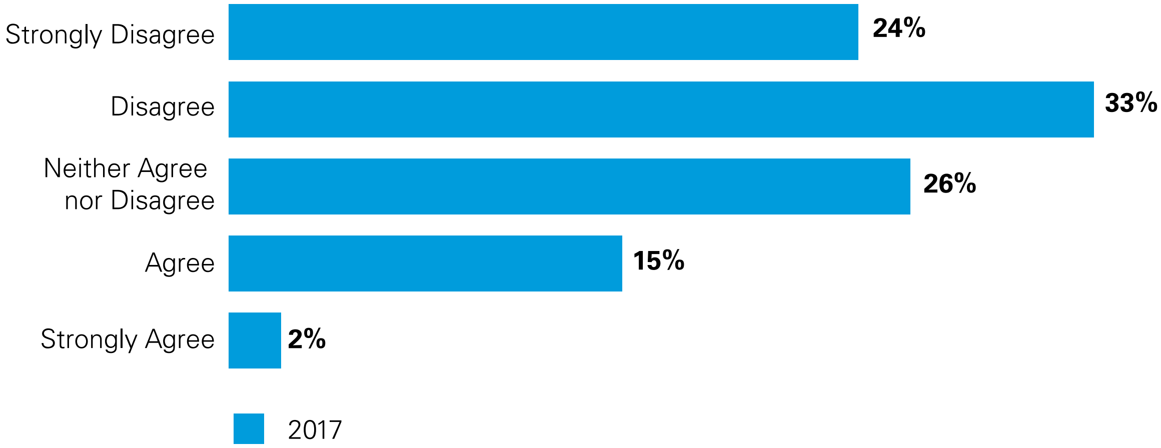
Q: My organization provides sufficient risk management training for staff to effectively and efficiently carry out their risk management responsibilities.



Source: 2017 Federal Enterprise Risk Management Survey, PwC and AFERM.

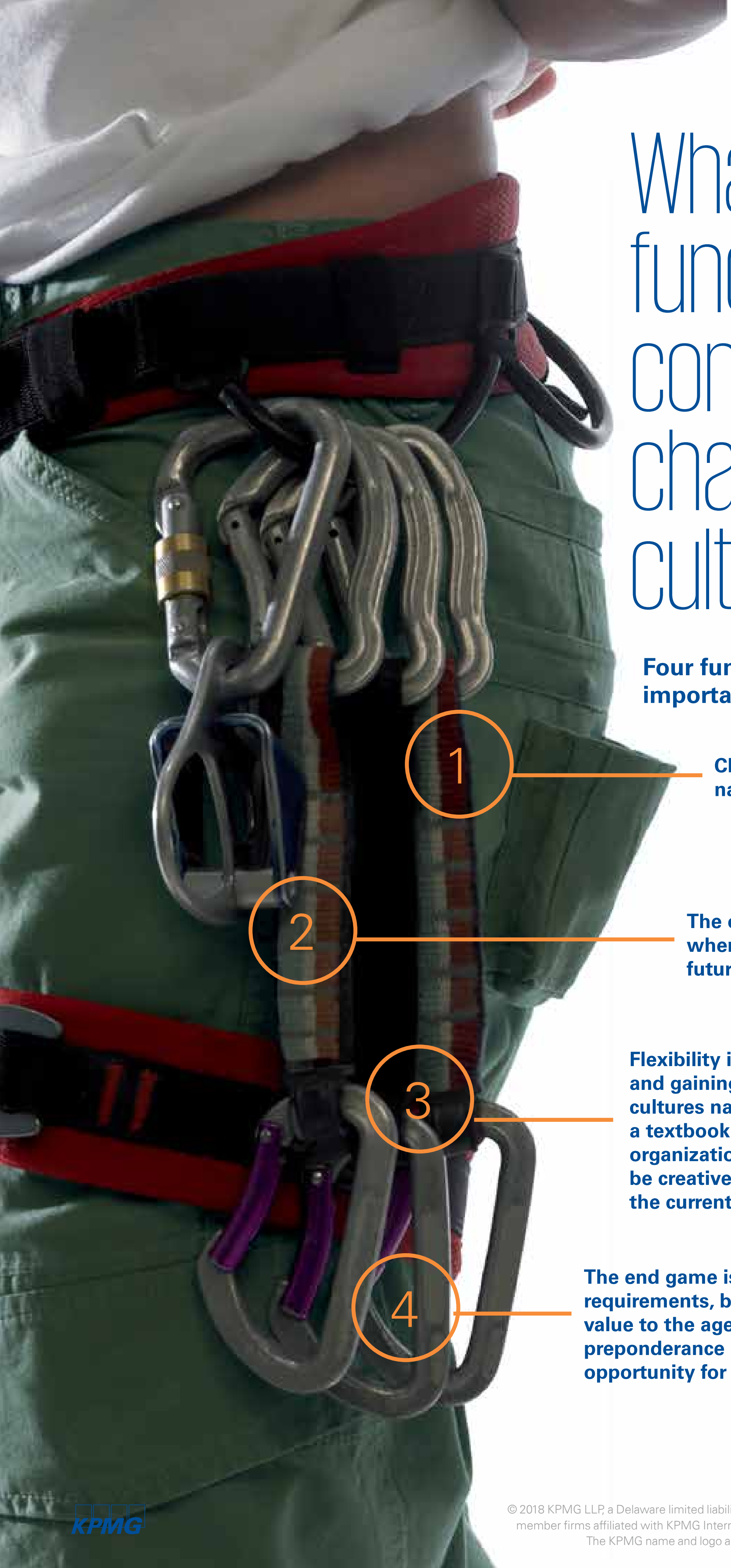
Figure 7: Survey question

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.



Source: 2017 Federal Enterprise Risk Management Survey, PwC and AFERM.

The bottom line is that, while culture is a determinant of ERM program success, it is presently the largest barrier and will remain so without a concerted and sustained transformation effort.



What are the fundamental considerations in changing the risk culture?

Four fundamental considerations provide important context to the task at hand.

Change is personal and people have a natural need to know why.

The organization has to thoroughly understand where it wants its risk culture to be in the future and where the risk culture is now.

Flexibility is vital in moving culture in a new direction and gaining acceptance for change. Wide variances in cultures naturally exist and always will. There is not a textbook answer or one solution that works for all organizations. As such, federal agencies will have to be creative and leverage risk management aspects of the current culture to move to a new culture.

The end game is not compliance with OMB's ERM requirements, but rather an approach that adds value to the agency in carrying out its mission. If the preponderance of the focus is on compliance, the opportunity for meaningful change can quickly dissipate.

1 Change is personal and people have a natural need to know what and why

The changes envisioned in moving to ERM go far beyond tweaking agencies' existing internal control programs under the Federal Managers' Financial Integrity Act of 1982 (FMFIA)[8] and the earlier versions of OMB Circular A-123. They will involve openness and transparency that may run against the grain of an agency's existing culture.

Change is personal: People can react to change differently. Some may be genuinely enthusiastic and immediately jump on the bandwagon to add their talents to making the change work for betterment of the organization. They are excited by the prospect of making a positive difference and wonder why it did not happen sooner. To others, there may be so much anxiety and fear about the unknown, they do the bare minimum possible to help with the change initiative and are inwardly rooting for the status quo to prevail. Some may be deeply skeptical as to whether the change will actually add value and instead spend their energies on pushing for a different set of changes. For some, there may be distrust of management's intentions and opposition and hostility directed at undermining any changes to the status quo.

A person may go through all or just some of these phases and may do so more than once during a change initiative. Building trust becomes key, because change is ultimately a personal choice. It is important to keep in mind that change in highly successful organizations can be more difficult than in organizations that are not as successful. The question may be "Why rock the boat? We are doing great."

People have a natural need to know what and why: At the outset, people will expect top management to be able to answer fundamental questions, such as:

— Why are we doing this?

— How will this improve the achievement of the mission?

— What will be the impact on me personally?

— How will this be implemented and over what time frame?

— What is the end game?

— How do we get there?

Some people quickly gravitate to any change, even if it is just saluting the flag and having a positive attitude. But most have to understand and be convinced at some level of specificity. Then, the central premises supporting change have to be continually reinforced and adapted as needed throughout the process. There is no magic wand. Expect some skepticism, malaise, or even hard push back at the outset and perhaps throughout the change process.

Therefore, leading organizations are totally transparent with staff on why they support ERM and its end game. When people fully understand the goal and the rationale, they are more likely to trust top management and be supportive. Staff will also have to see how stalwartly top management is on board with and committed to ERM. Management must clearly "walk the talk" as well as own ERM and the cultural transformation that is entailed. Leading organizations demonstrate highly visible top management ownership, recognizing that simple sponsorship is not enough.

[8] Public Law 97-255, September 8, 1982.

2 Leading organizations thoroughly understand where they want the culture to be in the future and where they are today

Having a fundamental understanding of the current state and desired future state of the risk culture enables organizations to leverage a conceptual framework centered on eight cultural risk drivers, which will be addressed later in this white paper.

Identifying the desired risk culture provides a benchmark for the future

A fundamental component of ERM is clearly identifying the risk management objectives and the desired risk culture to support those objectives. Leading organizations define their risk appetite and risk tolerance at the outset and use them to anchor the program. They do so in the context of their strategic mission goals and objectives. This determination is both an art and a science. It requires broad involvement across the organization, outreach to stakeholders, and the personal attention of top management.

Think of it as getting answers to a series of questions, such as:

— What are the expectations of the public, the president, and the congress?

— Is the risk culture a strategic priority, and why should it be?

— How do risk management and the risk culture impact the effective and efficient achievement of the organization's strategic mission objectives? Government employees are committed to achieving missions in the public interest. Being able to clearly link ERM to an ability to improve mission delivery and/or reduce costs will help engender support around an ERM culture.

— How are core values and public expectations integrated into the mission, strategic objectives, decision-making processes, and accountability and transparency mechanisms? They represent important levers in defining and changing the risk culture.

— Are the definitions and specific expectations associated with core values clearly defined and articulated so there is common understanding across the organization?

— How is ERM different from and how does it intersect and support other "good government" management initiatives? It will be vital that ERM is not viewed as an unfunded compliance exercise, but is seen as an essential part of program management, such as establishing program integrity.[9]

Once top management has defined the risk appetite/tolerance that undergirds the ERM program and the desired risk culture, it is important to be transparent with staff on how it was established and what it means to them. Leading organizations get staff feedback and make them part of the process. It cannot be overemphasized that when people fully understand the goal and the rationale, they are more likely to be supportive.

Understanding the current risk culture provides the current baseline

Now that the agency has identified its desired risk culture, fundamental to change is understanding the current situation or the baseline starting point. Included are the formal processes and informal cultural norms as well as the levers, or facilitators that are most likely to move the organization to a new path.

Leading organizations:

— Identify gaps between the current and desired risk culture, which helps define change actions and inform prioritization.

— Identify current and potential barriers and enablers.

— Preserve and leverage what works within the current culture. While sometimes necessary, starting from scratch can present a much larger challenge. Where possible, they put the desired risk culture in terms familiar to the staff.

— Appreciate the nature of cultural inconsistencies and challenges within their organization and equip leaders and staff with insights and tools to navigate the situation.

[9] "Switching gears – Expanding program integrity beyond fraud, waste, and abuse to enhance mission performance," KPMG Government Institute, June 2018 (http://www.kpmg-institutes.com/institutes/government-institute/articles/2018/06/switching-gears--expanding-program-integrity-beyond-fraud--waste.html).

In understanding their agency's risk culture, both above and below the surface as shown on Figure 2, leading organizations get answers to questions such as these at the outset.

- What are the current motivations, beliefs, and assumptions that drive behavior?
- What are the current behaviors that contribute or detract from achieving the desired risk culture?
- Even where risk is known to be low, do management systems include so many controls that efficiency and even effectiveness are negatively impacted with little to no added positive impact on program delivery?
- What is the general attitude toward change?
- Is there an openness to doing things differently, including needed flexibility and innovation?
- Is there an ability to manage change though proven, stable processes?
- What is the level of empowerment and individual initiative?
- Are people and organizations interdependent, as demonstrated by broad collaboration and interaction across entities and groups, or do they operate independently as stove-piped silos?
- Is management willing to accept calculated risk through well-established risk appetites/tolerances that are universally understood and used in managing the organization?
- Are employees afraid to make a decision or accept risk, even if it is clearly within the agency's risk appetite/tolerance?
- Is there a reluctance to raise concerns and identify risks for fear of reprisal or not being viewed as a team player? Leading organizations have zero tolerance for reprisal in situations where employees come forward with their concerns and ideas.
- When problems arise, what happens?
  - Is top management immediately told?
  - Is there a capability to quickly react?
  - Is there accountability and transparency?
  - Does the organization learn from mistakes that are outside its risk appetite?
- Are jobs "hard wired," whereby people are not expected to think beyond their own responsibilities? Any changes to those responsibilities may be strongly resisted or more difficult to make, even if people are somewhat open to change.

Leading organizations also strive to continually keep their finger on the risk culture pulse through:

- Public surveys focused on service and mission delivery
- Regular employee feedback surveys
- Top-management visits and employee outreach
- Well-targeted metrics and culture dashboards
- Well-focused business change cases that incorporate employee input
- Confidential citizen and whistleblower hotlines
- Senior risk officers who serve as risk facilitators
- Benchmarking against leading organizations
- Research around risk drivers and emerging risks
- Monitoring social media
- Asking tough questions, within and outside the organization
- Seeking outside counsel and other expertise where needed
- Timely and transparent action to address risks and/or bad behavior
- Auditor input, given the wealth of knowledge auditors gain across the enterprise.

3 Flexibility is vital to moving culture in a new direction and gaining acceptance for change

In the federal government, organizational cultures can widely vary, such as cultural differences between civilian agencies and Department of Defense (DoD) agencies. Even between and within civilian and DoD organizations as well as within professional disciplines (whether program management, information management, human capital management, procurement, financial management or the host of other discrete professions in government), the cultures may differ appreciably. Also, in interacting with state and local government and private sector stakeholders, there may be markedly different cultures.

This is not to imply there should be a universal culture or that one culture is better than the other. Cultures naturally differ and always will to some extent. It is a recognition of the important role of culture and how an organization and people may respond differently to risks and changes in the environment around them that create risks. Culture can be so powerful that top leaders must have a laser focus on first understanding and then adopting strategies to leverage and adapt the culture as needed.

Successfully moving to ERM involves changing the attitudes, values, goals, and practices around risk management across what can be large, diverse organizations, which themselves may include a range of different cultures. While there are a variety of views, scientific studies have shown that organizations which intentionally manage their cultures outperform similar organizations that do not.[10] The move to ERM will not happen overnight, requiring perseverance and continuing top management emphasis.

[10] For example, see "Enhancing Organizational Performance, Chapter 3, Organizational Culture," Daniel Druckman, Jerome E. Singer and Harold Van Cott, Editors, Committee on Techniques for the Enhancement of Human Performance, Commission on Behavioral and Social Sciences and Education, National Research Council (National Academy of Sciences, National Academy of Engineering, and Institute of Medicine) National Academy Press, 1997.

4 The end game of ERM is not simply compliance

OMB Circular A-123 does not speak of the end game in terms of compliance with its requirements, the Comptroller General of the United States' Standards for Internal Control in the Federal Government (Green Book),[11] or the provisions of FMFIA. Instead, effective risk management:

- Creates and protects value
- Is an integral part of all organizational processes
- Is part of decision making
- Explicitly addresses uncertainty
- Is systematic, structured, and timely
- Is based on the best available information
- Is tailored and responsive to the agency's evolving risk profile
- Takes human and cultural factors into account
- Is transparent and inclusive
- Is dynamic, iterative, and responsive to change
- Facilitates continual improvement of the organization.

These concepts drive leading ERM programs. In moving to ERM, it is important to avoid the implementation pitfalls of FMFIA. Especially in the early years of FMFIA implementation, agency cultures drove the primary focus to creating a paper trail documenting adherence with detailed OMB requirements versus addressing many of the more serious and complex management control and financial management weaknesses.[12]

Also, as a general proposition, organizations "get what they measure and reward." If the bottom line is essentially what matters and how results were achieved is not seen as important, risks and the potential for bad behavior typically increase. Similarly, if bad decisions have no or little real personal consequence, the risk of bad decisions will likely increase. If top management's focus is strictly short - term, long-term risks will likely be overlooked. If top management never asks how risk is being managed or is indifferent to the concept altogether, a strong risk management culture will be difficult to foster. If core values are lacking or are not enforced, the risk culture is negatively impacted.

At the same time, there can be downsides to having an overly-structured risk management system that requires strict adherence to dotting every "i" and crossing every "t" without focusing on the underlying risk. OMB Circular A-123 speaks to finding the right balance between risk and control: "Federal managers must carefully consider the appropriate balance between risk, controls, costs, and benefits in their mission support operations. Too many controls can result in inefficiencies, while too few controls may increase risk to an unacceptable level."

Countless rules, regulations, and controls do not necessarily equate to a "risk proof" organization. Organizations can become awash in policies and procedures that are so onerous they jeopardize mission accomplishment and waste resources. Too many controls, but not always the right ones, can result in an increase in undesirable results. People can simply become overly bogged down with rote compliance, without identifying risks and focusing on the most important risk drivers.

This can also lead to a mindset that compliance serves as a "get out of jail card" if something goes wrong. People might not see the need or learn to be "risk aware." Often referred to as the "airbag effect," there can be a false sense of security, and some people may drive faster and more carelessly as a result.

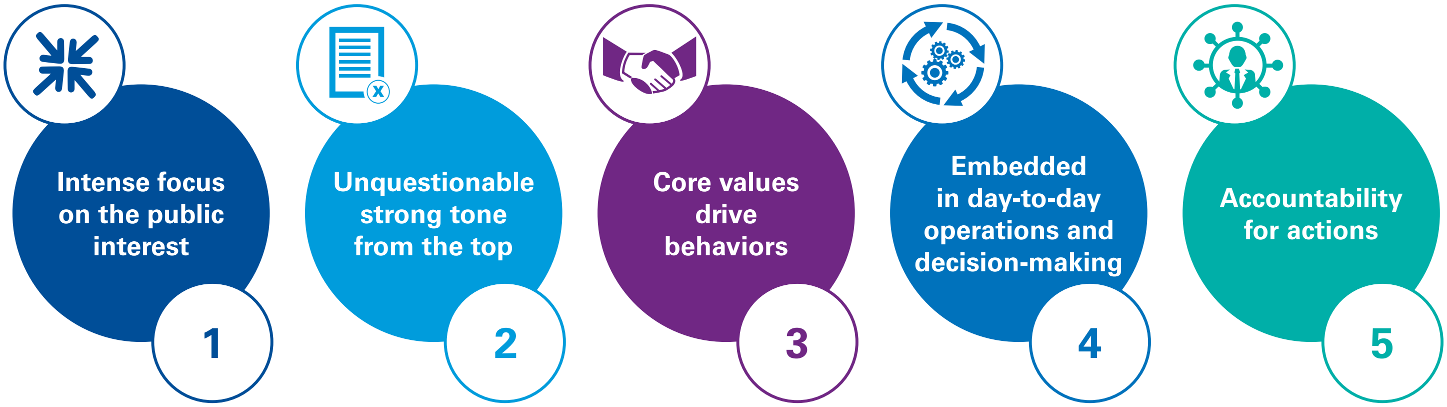
[11] The Green Book is issued by the Government Accountability Office (GAO) (https://www.gao.gov/greenbook/overview).

[12] "FINANCIAL MANAGEMENT – Effective Internal Control is Key to Accountability," Statement of Jeffrey C. Steinhoff, Managing Director, Financial Management and Assurance, GAO-05-321T, February 16, 2005.

What are the attributes of leading risk cultures in government?

Now that we have introduced the context around the four fundamental considerations in addressing organizational risk culture, we will examine five attributes of a leading government organizational risk culture. We identified these attributes based on having worked with organizations in the United States and globally that were faced with the movement to ERM or other transformation initiatives. The five attributes are highlighted in Figure 8 and discussed in the sections that follow.

Figure 8: Attributes of leading government risk cultures


Intense focus on the public interest
1
Unquestionable strong tone from the top
2
Core values drive behaviors
3
Embedded in day-to-day operations and decision-making
4
Accountability for actions
5

1 Attribute 1: Intense focus on the public interest

In government, an argument could be made that a strong risk culture focuses on "doing the right thing in the public interest in adherence to organizational core values in order to achieve mission and strategic objectives effectively and efficiently, with the highest level of integrity and public service." Government was established to address public needs and is accountable to the people. The public are not only customers, but shareholders, who invest through their tax dollars and provide their proxies to elected officials. Thereby, the risk culture and the public interest intersect.

Public trust in the government "to do what's right always or most of the time," has dropped considerably from 75 percent in 1964 and now hovers in the 20 percent range.[13] There are plenty of reasons for this, but as we all know, once lost, trust is more difficult to regain. As Benjamin Franklin said: "It takes many good deeds to build a good reputation, and only one bad one to lose it."

Government is expected to accomplish not only the easy tasks, but those that are the most challenging and under the most difficult conditions, such as defending the nation and disaster relief. A risk culture of integrity and service in the public interest is paramount. Expectations of what this means can vary greatly given the diverse views on the role of government and the needs of citizens. But since public resources are involved and government often steps in when other options are not available, the standards of behavior and performance are naturally high.

[13] "Public Trust in Government Remains Near Historic Lows as Partisan Attitudes Shift," Pew Research Center U.S Politics & Policy, May 14, 2017.

As stated in OMB Circular A-123: "ERM represents forward-looking management decisions, balancing risk and returns, so an Agency enhances its value to the taxpayer and increases its ability to achieve strategic objectives." This can be complicated in government. For example, in a survey by the Pew Research Center, 89 percent of respondents said the federal government should have a major role in responding to natural disasters, for which 64 percent (versus 79 percent in 2015) said the federal government is doing a good job.[14] However, what is a reasonable expectation for responding to a natural disaster, and where should management set its risk tolerance?

Among the basic expectations of the public are:

- Mission excellence, whether it be protecting the nation or delivering a social program that makes a difference to lives of Americans
- Customer service, including electronic interface with government and an ability to readily address questions and problems
- Responsiveness to current public needs
- Anticipation for and preparation to rapidly respond to emerging needs and risks
- Efficiency and effectiveness of programs and operations
- Prudent spending, with full accountability and transparency for tax dollars
- Accountability and transparency for results
- Protection of public assets and resources.

Leading government organizations calibrate their risk culture on effective and efficient service to the public, and they continually anticipate and plan for emerging risks that impact mission delivery. Focusing ERM on the public interest and the range of citizen expectations helps government agencies achieve strategic goals and objectives and build needed public trust. It also focuses ERM on issues of relevance that resonate with agency staff carrying out the mission as opposed to being focused on compliance with an OMB or another requirement.

2 Attribute 2: Unquestionable strong tone from the top

It bears repeating that the tone at the top represents what top management truly cares about and how they communicate their priorities and values, so they become part of the organization's DNA. Any change in the status quo, such as the changes to Circular A-123 and earlier changes in 2014 to the GAO's Green Book, are meant to be transformative. People will take top management's lead, but only if there is demonstrated commitment and clear direction. Leaders must always be role models for the right behaviors. As stated earlier, the 2017 ERM Survey found that 59 percent of the respondents view executive-level buy-in and support as barriers to establishing a formal ERM program. For respondents from organizations that had not yet established a formal ERM program, 85 percent saw the tone at the top as a barrier.[15]

These results are troubling since ownership by top leadership is vital to success in federal agencies that generally have many priorities and perhaps limited capability to address everything on their plates. In organizations considered "advanced" in implementing ERM, we have observed that senior management leads by example by making risk management a clear priority and driving appropriate risk management behavior.

In leading organizations, top management understands that successfully implementing an ERM program is not about issuing a memorandum, sending an e-mail to all staff, having a town hall meeting, or any combination of the above. Staff will need to see a sense of urgency and clear expectations that (1) focus on adding value through ERM versus rote compliance with OMB's and GAO's requirements, (2) are relevant to the agency mission and what people care about and should be doing day-to-day in their jobs, and (3) include clear recognition for success and accountability for failure to embrace risk management.

[14] "Government Gets Lower Ratings for Handling Health Care, Environment, Disaster Response," Pew Research Center U.S Politics & Policy, December 14, 2017.

[15] See footnote 3.

Consider these questions to help gauge the ownership by top leadership:

- Is top management fully invested in the role of ERM and concepts that represent sound risk management systems, so this commitment eventually permeates through the organization and becomes embedded in the culture? As stated earlier, in leading organizations, management "walks the talk" and visibly demonstrates clear ownership of risk management. They recognize that sponsorship is not enough?
- Does top management instead view the changes in Circular A-123 and the Green Book as an unfunded requirement or a new compliance exercise that is essentially the purview of the chief financial officer (CFO) and/or the inspector general (IG)? This is a recipe for failure since ERM is intended to be the responsibility of all agency organizations and all leadership and staff. The CFO and IG can certainly help facilitate sound risk management in their spheres of influence, but it is really everyone's job, with those involved in executing agency programs and operations most responsible.
- Does top management agree in concept with the value of moving ahead with ERM, but has higher priorities and is not willing to invest the time and effort in the program? As a result, there is no real top management engagement.
- Or do the changes to Circular A-123 and the Green Book not even make it to top management's radar screen? That may well be the case given the large percentage of respondents to the 2017 ERM Survey who saw the tone at the top as being an ERM barrier.

Appendix 1 includes a case study that examines what is possible when top leadership is laser focused on changing the risk culture. We highlight the Alcoa story and the transformational leadership of its chief executive officer, Paul O'Neill, former Secretary of the Treasury and OMB Deputy Director.

3 Attribute 3: Core values drive behaviors

Core values play an important role in the risk culture equation. Properly structured and implemented, they drive the behaviors that constitute day-to-day management, operations, and decision - making. They represent what the organization stands for and strives to achieve in the public interest. It would be hard to find a government organization that did not have stated core values. You will typically see words such as integrity, trust, honor, public accountability, reliability, respect for others, service, commitment, working together, open, honest, vigilant, community, excellence, selflessness, loyalty, courage, and excellence. A common denominator is "acting with integrity."

In leading organizations, everyone understands that they're accountable for creating a positive work environment, respecting those they work with, and supporting one another. There is a strong commitment to and pride in the core values at every level. It is about helping everyone in the organization make good choices and do the right thing in the right way in the public interest. Across the organization, people understand the core values and typically strive to live them day-to-day, not just in their professional lives but in their personal lives.

But even in leading organizations, do people see risk management as a component of core values and vice versa? Does top management even try to make that connection? Connecting the dots between risk management and core values provides direct context as to why risk management is important to the mission and what the organization and its people most value.

We all know that when risk is not properly managed, bad things are more likely to occur, and the impact is likely to be more serious. Such breakdowns cause the public to question whether the organization and its people really act with integrity and the other concepts engrained in most federal agency core values. Providing a link between core values and ERM provides positive reinforcement for the importance of effectively and efficiently managing risk and establishing strong program integrity.

An organization's people can be the best source of intelligence as to risks. But are they incentivized to come forward, or are they concerned about adverse repercussions to their career? A leading practice is to instill as an organizational core value that everyone is expected to "raise their hand" if they see problems, risks or wrongdoing, without fear of retaliation for speaking up. As stated in OMB Circular A-123, "ERM is beneficial since it addresses a fundamental organizational issue: the need for information about major risks to flow both up and down the organization and across the organizational structures to improve the quality of decision-making. ERM seeks to open channels of communication so the managers have access to the information they need to make sound decisions."[16] In leading organizations, the culture supports people for doing so, and even rewarding them when merited.

In many organizations, both in government and the private sector, the opposite may be true. The National Business Ethics Survey (NBES), which provides the U.S. corporate benchmarks on ethics, found that 63 percent of those observing misconduct in private companies reported the misconduct, of which 21 percent said they faced some form of retaliation.[17] OMB speaks directly to this in its Circular A-123: "Successful implementation of this Circular will require Agencies to establish and foster an open, transparent culture that encourages people to communicate information about potential risks and other concerns with their superiors without fear of retaliation or blame."[18] Encouraging employees to "raise their hand" without fear of retaliation not only benefits the organization as a whole, but also increases employee loyalty to the organization and its core values.

4 Attribute 4: Risk management embedded in day-to-day operations and decision - making

Mature ERM programs that are embedded into the organizational culture create sustainable value that directly supports day-to-day operations and decision - making. OMB Circular A-123 cites this as a component of the end game of ERM. Similarly, the GAO Green Book states that "In a mature and highly effective internal control system, internal control may be indistinguishable from day-to-day activities personnel perform." What this means is that internal control and risk management are second nature and seen as a normal part of routine operations.

It will take time for ERM programs to be fully mature. It is one thing to implement an ERM program to meet a requirement. It is another to fully integrate ERM into the fiber of everyday activities, whereby it becomes second nature. When organizations speak about the July 15, 2016 revisions to OMB Circular A-123 as being an unfunded mandate or address ERM as a compliance requirement, the journey to the end state becomes more difficult, and the results possible may never be fully realized.

As shown in the Alcoa case study in Appendix 1, there was a sense of urgency and meaningful results in a relatively short period of time by focusing on those risks of greatest importance to the company. A change in culture embedded change into the heart of the company, so that safety risks were center stage at all times to add value to both Alcoa's workers and the company.

[16] See footnote 1.
[17] The 2013 NBES is the eighth in this series since 1994.
[18] See footnote 1.

5 Attribute 5: Accountability for actions

In your organization, is there accountability for not taking reasonable actions to manage risks? What happens when corrective actions on identified problems linger for years and years? For example, some areas have remained on GAO's High-Risk List since the first High-Risk Series report in 1990,[19] and GAO and the inspectors general continually report thousands of open recommendations.

Leading organizations take appropriate and timely action when risks are not properly managed in line with the risk appetite/tolerance and consistent with core values. This does not necessarily mean that every time there is a significant problem someone is personally blamed and disciplined. The facts and circumstances become paramount in weighing accountability. But, having an accountability mind-set as part of the organization's risk culture demonstrates to everyone the seriousness of this responsibility.

In leading organizations, the expected results and behaviors are clearly defined in the performance management system, and staff are supported by the authorities and resources needed to achieve the expectations. Staff are rewarded for results and held accountable when there are shortfalls and/or problems that could have been reasonably avoided. A clearly avoidable problem could result in removal, downgrading, or reassignment of personnel based on the severity of and the facts and circumstances that led to the problem. There is always a delicate balance, and fairness and equity are paramount.

In organizations which do not have clear staff performance expectations and accountability mechanisms, mission failures, ineffectiveness, inefficiency, and/or instances of fraud, waste, and abuse can become characterized as simply a "system problem." An agency may not be able to hold any person(s) or organization(s) accountable in these situations. A culture of papering-over problems may manifest, resulting in continuing shortfalls in program results and public dissatisfaction with performance.

Also, in leading organizations, the culture is such that staff who raise concerns feel that their views are valued by management. When problems occur, which can be expected in any organization, people are then more willing to immediately raise the problem without fear that the messenger will be blamed or that top management will simply circle the wagons and not do the right thing. This requires a culture that includes strong trust and two-way respect between management and staff.

Finally, sound ERM concepts are adopted and enforced without regard to the person's level or position. If anything, risk management expectations of management should be even higher than staff, since management is ultimately responsible for staff performance and mission results. As President Harry Truman famously said: "The buck stops here."

[19] "High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others," GAO-17-317, February 15, 2017 (https://www.gao.gov/products/GAO-17-317).

How do organizations address gaps in their risk culture?

With an understanding of the gaps between the current and desired risk cultures, an organization is now positioned to begin changing the existing risk culture. We have identified eight transformation drivers, which have been paired and aligned under four aspects of cultural transformation. These drivers can be especially useful where risk management has not traditionally been viewed as everyone's core responsibility and/or has not been a management priority.

A conceptual framework to change the risk culture

Figure 9 presents the eight transformation drivers—clarity, visibility, involvement, role modeling, practicality, openness, enforcement, and improvement—and how they are organized under the four aspects of cultural transformation:

1. **Knowledge and understanding:** Each individual needs to know and understand what is expected of them and how their individual risk behavior links to the organization's overall performance. Top management must engage, listen, and communicate.
2. **Belief and commitment:** Everyone must believe in the added value of risk management and be committed to their organization's risk appetite and risk management approach.
3. **Competencies and context:** Similarly, everyone must understand the organizational context of risks and develop sufficient competent skills to ask relevant questions and weigh in as appropriate.
4. **Action and determination:** Timely actions are taken to address the root cause(s) of risk exposure in an organization. If the three aforementioned aspects are in place, individuals will more likely act in accordance with the agency's risk strategy and collectively develop the right risk culture. At the same time, mistakes, near misses, and even outright failures are a normal part of the process. People need to be empowered to take action, learn from mistakes, and know that the organization is determined to execute the agreed-upon risk strategy.

Figure 9: Risk culture conceptual framework

Cultural Aspects	Transformation Drivers	
Knowledge & Understanding	**Clarity** Is the ERM program well defined with clear and complete policies and procedures that are understood across the organization? Do individual employees understand what is expected and their specific role?	**Visibility** Is employee behavior with respect to risk management (for example, the risk responses and the effects thereof) visible to the organization?
Belief & Commitment	**Involvement** Do employees feel accountable for the proper application of risk policies and take ownership for the organization's risk strategy?	**Role Modeling** Does management lead by example and display leadership, especially regarding risk management?
Competencies & Context	**Practicality** Do the organization's actions correspond to the risk appetite/tolerance and overall risk strategy? Are employees enabled to do what is requested of them in terms managing risks?	**Openness** Is it normal to regularly discuss risks, both current and potential, with an atmosphere that encourages staff at all levels to raise their hand when they see a problem, and then challenges current assumptions and practices while fostering mutual respect?
Action & Determination	**Enforcement** Are employees rewarded for responsible behavior? Is irresponsible behavior disciplined?	**Improvement** Are incidents and near misses evaluated to determine potential risks? Do employees feel they learn from mistakes?

A series of statements support application of the framework

Building on the above descriptions of each of the four aspects and the underlying questions that frame each of the eight transformation attributes, we have developed a series of statements for use in applying the transformation framework. The statements are included in Appendix 2: Applying the Risk Culture Transformation Framework—Can the organization say "yes" to these statements? The ultimate goal is to be able to say "yes" to all applicable statements. It is expected that, where applicable, actions will be taken to address areas where the answer is either "no" or "uncertain."

For example, under transformation driver 6, Openness, there are 11 statements including the following:

- There is openness to doing things differently, including needed flexibility and innovation.
- When issues arise, they are openly and professionally discussed in the organization, with a view of collectively solving the problem.
- Top management and staff are mindful of changes in the environment that could introduce new risks and/or exacerbate existing risks to a level that is beyond the organization's risk appetite/tolerance and freely exchange their perspectives up and down the organization.

Our experience has been that organizations often struggle with the type of risk culture issues covered by the statements in Appendix 2. For example, while management may think there is openness to risks, problems, concerns and ideas, the staff may not at all see it that way. In this regard, OMB has emphasized the importance of "open channels of communication so the managers have access to the information they need to make sound decisions." As stated earlier, OMB Circular A-123 also expressly calls on agencies "to establish and foster an open, transparent culture that encourages people to communicate information about potential risks and other concerns with their superiors without fear of retaliation or blame."[20] The culture must accommodate that thinking. Agencies would, therefore, frame their risk culture transformation plan around what it would take to be able to say "yes" to the statements in Appendix 2. This would necessitate the active engagement of top management.

Assessing the culture – Survey results

Leading organizations continually strive to maintain a holistic understanding of their risk culture and whether it is appropriate, adequate, and effective for what can be a changing risk environment. They use the leading practices captured in the Appendix 2 questions as a guide post in conducting surveys, interviews, and focus group sessions and in considering reports of risk incidents and near misses.

Figure 10 includes a high-level example of the type of information that may be gained by applying the questions in Appendix 2 to each of the eight cultural drivers with "clarity" highlighted as an example. Answers to the questions would result in a numeric a score for each drive, together with detail as to what contributed to the score.

[20] See footnote 1.

Figure 10: Example of survey result information

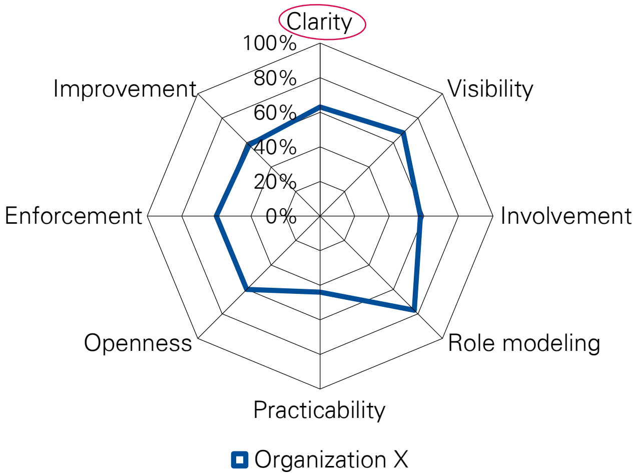
All outcomes of the survey are collected per cultural driver and translated into negative, neutral, and positive.

Negative = Fully disagree + Disagree

Neutral = Partly disagree/partly agree

Positive = Fully agree + Agree

The average positive outcome of all questions, represent each cultural driver. All outcomes are represented in a report via a table with all questions, a table with an overview of all cultural drivers and a spider web of all cultural drivers.



Clarity (63%)	**Organization X**		
	Negative	**Neutral**	**Positive**
I am confident that I could describe the benefits of having a risk management policy	8%	12%	80%
The level of understanding of the department's policy for managing risk is high within my department	40%	5%	45%
The management's appetite for allowing to take some risks is clear to me	30%	6%	64%

Cultural drivers	**Results Organization X**
Clarity	63%
Visibility	68%
Involvement	58%
Role modeling	77%
Practibility	44%
Openness	60%
Enforcement	60%
Improvement	58%

From this type of information, organizations can gain a better understanding of their risk management strengths and weaknesses. This can provide intelligence on where to focus corrective actions targeted to root causes and risk culture implications.

Final thoughts

ERM has to be owned, understood, and implemented by everyone in the organization, starting at the top. It has to be viewed as a vital element of program and operational management and not a compliance exercise. A common theme in this white paper is that leaders and all staff will have to be motivated to do the right thing and recognize the critical importance of instilling a positive risk culture in the fiber of the organization, so that it becomes a facilitator and not a barrier to ERM. Risk management should be something that happens naturally and adds clear value to effectively and efficiently accomplishing the mission and instilling public trust in government.

That motivation will have to be sustained and reinforced between administrations, given the transformational nature involved in changing the risk culture. Top management leadership must continue to be visible, passionate, and engaged to break down the cultural barriers identified in the 2017 ERM Survey.

Across organizations, there will need to be a high degree of:

- Knowledge and understanding through clarity and visibility around the value of risk management, what is expected, and the behavior of leadership and staff as it relates to risk management.
- Belief and commitment by leadership and staff, who must own risk management as demonstrated through their involvement and leadership by example as role models.
- Competency and context, whereby actions correspond to the organization's risk appetite/tolerance and overall risk strategy. Leaders and staff must be empowered to do what is necessary to manage risks in an environment that is open and transparent and values everyone speaking up. The organization will need to be willing to challenge the status quo and do things differently by attacking barriers to strong risk management programs.
- Action and determination by rewarding employees for responsible risk management and holding people accountable for irresponsible behavior that disregards risk management tenets, leading practices, and the expectations of top management. There will need to be a continual focus on improvement by learning from mistakes and adopting leading risk management practices.

ERM is not about nibbling at the edges, but looking holistically at programs and operations from a different lens. As Albert Einstein said: "We can't solve problems by using the same kind of thinking we used when we created them." Reflecting on achieving agency missions in times of continuing fiscal challenge and a widespread lack of public trust, there is a need to recognize the power of culture in identifying and strategically addressing risks. Through strong risk management as an enabler and not a barrier, organizations can seize opportunities to enhance program results and service delivery to the American public, while reducing costs and gaining greater public trust.

Appendix 1:

What is possible with a strong risk culture?

Let's examine the dramatic results that can be achieved when a strong risk culture is established by top management and driven throughout the organization as a guiding principle.[21] When Paul O'Neill, who subsequently served as the Secretary of the Treasury and had previously served as OMB's Deputy Director, became the chief executive officer (CEO) of the Alcoa Corporation in 1987, his driving mantra was worker safety. He did not talk about boosting Alcoa's profits or company value, which is what the financial markets expected to hear from a CEO. He told market analysts and Alcoa's Board to just look at the safety of Alcoa's workers to gauge the company's performance.

Alcoa's safety record, measured based on average employee days lost to on-the-job injury annually, was better than national norms, and Alcoa was in a manufacturing industry where the risk of injury is higher than the norm. This made the focus on safety even more puzzling to some. O'Neill was quoted as saying: "I intend to go for zero injuries."

His personal commitment to this goal was evident as he changed the culture by engaging Alcoa employees at every level of the organization. He not only conceived of the new normal for worker safety and talked about it, but walked the talk and made sure the organization understood the importance of and his personal commitment to the program. In a 2002 speech to Harvard University MBA and Kennedy School of Government students, "I was prepared to accept the consequences of spending whatever it took to become the safest company in the world."[22]

Work days lost to injury plummeted from almost two days per worker per year to less than two hours a year and subsequently went even lower. Safety initiatives resulted in manufacturing changes and continuous improvements in all operations and processes, made possible through heightened worker engagement and partnership with top management. He valued worker input on safety and better ways of doing their jobs. Being safer meant being more efficient and effective and making investments that not only protected the workers but improved manufacturing processes and operations.

A year after Paul O'Neill joined Alcoa, profits hit a record high. At the time of his retirement from Alcoa in 1999 to serve as the Secretary of the Treasury, the company's reported market value had risen from $3 billion to $27 billion, reported annual revenue went from $1.5 billion to $23 billion, and reported annual net income had gone from $200 million to almost $1.5 billion.[23]

The Alcoa story demonstrates what's possible when an organization focuses on risk from an enterprise perspective and drives clear change to the risk culture from the top. There was a higher purpose of worker safety and recognition that cultural and operational changes were necessary to seize opportunity. The leader was steadfast in his demands to be the safest company and his conviction that this would lead to success. Senior leaders were held accountable, and injuries were analyzed and immediate corrective actions taken. Ultimately, the focus on risks to worker safety also translated into immense bottom line profitability and company value.

Inducted into the Manufacturing Hall of Fame in 2012, Paul O'Neill was quoted as saying: "In order to create a high-performance organization, you have to have values that are acted on, beginning with giving real meaning to the idea that people in the organization are the most important asset… I thought if we could live by the idea that we could strive every day to be the best in everything we do, then by definition we would have great financial success."[24]

[21] Paul O'Neill and the Alcoa Story were earlier discussed in "It's Time to Seize Opportunity," by Laura A. Price and Jeffrey C. Steinhoff, AFERM Updates, Issue 20, December 2016.

[22] "Paul O'Neill: Values into Action," Harvard Business School, Working Knowledge, by Martha Lagace, November 4, 2002.

[23] Ibid; and "The Power of Habit: Why We Do What We Do in Life and Business," chapter titled "The Power of Safety Leadership: Paul O'Neill, Safety and Alcoa," by Charles Duhigg, February 2012.

[24] "Manufacturing Hall of Fame 2012 Inductee: Paul O'Neill," by Travis M. Hessman, IndustryWeek, December 17, 2012.

Appendix 2:

Applying the transformation framework to the risk culture—Can the organization say "yes" to these statements?

Knowledge and understanding

1. **Clarity:** Is the ERM program well defined with clear and complete policies and procedures that are understood across the organization? Do individual employees understand what is expected and their expected role?

— Staff at all levels are well aware the organization has adopted risk management policies and procedures and the priority management places on risk management.

— Staff understand the benefits of risk management in the context of the mission performance.

— Staff understand the requirements of the organization's overall risk management policy.

— Staff understand how the risk management policy intersects with and compliments the organization's core values.

— The level of awareness and understanding of the organization's more detailed risk management processes and procedures are commensurate with a staff member's roles and responsibilities.

— Staff understand their specific role and responsibilities for risk management.

— Formal overall risk management responsibilities have been assigned to someone in the organization, and staff understand who they can go to for advice.

— Risk information is effectively communicated up and down the organization.

— Staff understand management's appetite/tolerance for risk and know the bounds of their own authority and what should be avoided.

— Staff understand the end game of risk management is support to mission excellence and not compliance with OMB Circular A-123 or checking boxes that something has been completed.

— Risk management is widely viewed and consistently understood throughout the organization as:

  - Systematic, structured, and timely
  - Transparent and inclusive
  - Dynamic, iterative, and responsive to change
  - Part of day-to-day operations and decision - making that constitute mission execution.

2. **Visibility:** Is employee behavior with respect to risk management (for example, the risk responses and the effects thereof) visible to the organization?

— Employee motivations, beliefs, and assumptions driving behavior are understood by top management.

— Risk is formally considered in making key decisions through business cases and other processes used by management and that consideration is documented.

— Risk is a general consideration in all day-to-day decisions and activities.

— Local managers and supervisors know how their employees manage risks.

— The organization keeps its finger on the pulse and realizes when things begin to go wrong.

— Local managers and supervisors know what type of behavior really goes on within the organization.

— The opportunity to engage in misconduct is minimal.

— Assessments to detect new or increased risks are timely and comprehensive.

— New risks or significant changes to existing risks are timely and clearly communicated to everyone with a need to know.

— There is continuing evaluation of operating practices, key controls, and new risk management initiatives.

— Staff believe that internal controls are difficult to bypass or override, but are cognizant of the risk of lacking key controls or having too many controls that do not provide value in line with the organization's risk appetite/tolerance.

— Staff awareness is high in cases where things just do not look right on the surface.

Belief and commitment

3. **Involvement:** Do employees feel accountable for the proper application of risk policies and take ownership for the organization's risk strategy?

- In the context of risk management, there is intense focus at all levels across the organization on supporting:
  - Mission excellence
  - Customer service
  - Responsiveness to current public needs
  - Anticipation for and preparation to rapidly respond to emerging needs and risks
  - Prudent spending, with full accountability and transparency for tax dollars
  - Accountability and transparency for results
  - Protection of public assets and resources.
- Across the organization, everyone is engaged in risk management as an integral part of day-to-day responsibilities, without regard to placement or level in the organization.
- Staff understand what is required and have an opportunity to weigh on any facet of the risk management program, engendering broad-based support.
- Staff understand that they individually and collectively own the risk management program and are accountable for its effective an efficient implementation.
- The organization adopts and enforces leading risk management practices, while recognizing the importance of providing staff needed flexibility and agility within the risk appetite/tolerance.
- Managing risk is seen as an important factor in how individual work activities are planned.
- The right people (including staff outside an individual's immediate work unit if necessary) are involved in managing the risks that affect the organization.
- Staff believe their input will be valued and considered by top management.
- A culture of "smart" compliance with policies and procedures exists so that staff see clear value and support risk management.
- The risk management approach is seen as important to getting the right mission results and protecting the public interest.
- Staff believe they have both accountability and responsibility for risk management, as well as the tools and support to do what is necessary.

4. **Role modeling:** Does management lead by example and display leadership, especially regarding risk management?

- The top leadership team continually demonstrates a commitment to effectively and efficiently managing risks through their words and actions.
- Top management exemplifies the core values.
- There is clear executive sponsorship of and direct involvement in embedding the risk management framework in the organization and its day-to-day operations.
- The agency head and other senior political and career executives have demonstrated a collective view regarding the risk appetite/tolerance, which has been clearly communicated to everyone and is periodically reinforced.
- Management at all levels lead by example when it comes to managing risks.
- Staff feel their views and perspectives are valued by management.
- Management at all levels drive a culture which encourages employees to identify and report control breakdowns and potential risks as a fundamental part of their job.
- Staff feel empowered to freely escalate risks and bad news.
- There is absolutely no tolerance for real or perceived retaliation when people have stepped forward and done the right thing in raising current and potential problems and risks to management.
- Staff have a clear understanding of top management's desired risk culture.
- Staff believe top management sets the right tone on the importance of the risk culture.
- Staff believe their direct manager sets the right tone on the importance of the risk culture.
- Staff are unafraid to take risks within the established acceptable risk appetite/tolerance, which considers both potential negative impacts and potential rewards.

Competencies and context

5. **Practicality:** Do the organization's actions correspond to the risk appetite/tolerance and overall risk strategy? Are employees enabled to do what is requested of them in terms of managing risks?

- The level of calculated risk that management is willing to accept is universally understood and applied by staff.
- Risk management policies and procedures are directed at adding value and not overburdening staff with compliance requirements that take their eyes off of what is really important in managing risk and executing programs.
- Staff have sufficient tools, including automated monitoring tools where applicable, to enable them to manage the risks that arise in their job.
- As needed, staff have access to additional expertise to help manage risks.
- There is sufficient and continuing risk management training for staff to effectively and efficiently carry out their risk management responsibilities.
- When problems arise:
  - Management is immediately alerted.
  - Management is there to assist.
  - There is a capability to react quickly
  - Accountability and transparency are evident.
  - The organization learns from mistakes.

6. **Openness:** Is it normal to regularly discuss risks, both current and potential, with an atmosphere that encourages staff at all levels to raise their hand when they see a problem, and then challenges current assumptions and practices while fostering mutual respect?

- Management at all levels are viewed as open and trustworthy.
- There is openness to doing things differently, including needed flexibility and innovation.
- When issues arise, they are openly and professionally discussed in the organization, with a view of collectively solving the problem.
- Management and staff are mindful of changes in the environment that could introduce new risks and/or exacerbate existing risks to a level beyond the organization's risk appetite/tolerance and freely exchange their perspectives up and down the organization.
- Local managers and supervisors are approachable if staff have questions or concerns about risks.
- Without fear of retaliation, staff feel comfortable:
  - Reporting bad news
  - Identifying new risks
  - Sharing their concerns and opinions
  - Seeking advice about any facet of the risk management strategy
  - Working across organizational boundaries to raise and address risks
- Staff frequently report bad news, identify new risks, share their concerns and opinions, and/or seek advice, and view this as an expectation of management.
- Top management is accessible to staff and regularly seeks employee through a variety of formal and informal mechanisms, such as:
  - Visits and outreach
  - Regular employee feedback surveys
  - Town hall meetings
- The organization uses well-targeted risk management metrics and dashboards that are shared with staff and openly discussed.
- Cultural diagnostics are used to gauge on an ongoing basis the state of cultural values at all levels of the organization, both above and below the surface depicted in Figure 1.

Action and determination

7. **Enforcement:** Are employees rewarded for responsible behavior? Is irresponsible behavior disciplined?

- When something goes wrong, the organization understands that top management will:
  - Own the problem
  - Act with openness and transparency
  - Ask tough questions as needed
  - Immediately focus on identifying the root cause and addressing the underlying risk
  - Identify and take appropriate action to address the underlying risk
  - Take appropriate disciplinary action, where justified based on the facts and circumstances.
- Top management continually emphasizes the importance of the risk culture across the organization and the expectation that everyone be committed to risk management.
- Risk management objectives are included in individual performance goals at every level of the organization.
- When staff identify and report a violation of the risk culture to top management, staff are confident the matter will be properly handled and with appropriate confidentially.
- Staff feel free to report risks and violations of the risk management policies without fear of retaliation.
- Top management has no tolerance for any form of retaliation and has a track record of disciplinary action should such a problem occur.
- If staff reported a violation of the risk culture to management, they would strongly believe they were doing the right thing.
- The organization has made clear the actions that will be taken to hold staff accountable for not adhering to the risk appetite/tolerance or otherwise not executing their risk management responsibilities.
- Staff are clearly rewarded for managing risks in line with the risk appetite/tolerance established by top management.
- There is a strong link between risk management and performance.
- Staff feel accountable for adhering to the risk culture and doing everything reasonably practical to avoid situations that go beyond the organization's risk appetite/tolerance.
- Violations of core values by staff at any level in the organization are not tolerated and appropriate disciplinary action is taken.
- Action on audit recommendations does not languish on the back burner, with responsible management and staff held accountable for timely and effective corrective action.

8. **Improvement:** Are incidents and near misses evaluated to determine potential risks? Do employees feel they learn from mistakes?

- The organization monitors what happens day-to-day to identify and benefit in the future from incidents and near misses by learning from these situations and taking timely action to address identified risks.
- Excessive and/or ill-advised risks taking is immediately and thoroughly evaluated to determine root causes and develop corrective actions and mitigation strategies.
- The organization learns from problems that do arise.
- Top management recognizes there will be mistakes and views them as natural learning opportunities to be acknowledged and widely shared across the organization.

- Actions to reduce identified risks to a level consistent with the risk appetite/tolerance are effective, efficient, and timely.
- A culture of continuous improvement is evident to help prevent the reoccurrence of problems and to prevent future risks from becoming problems.
- The organization looks to other organizations for leading practices and lessons learned.
- There is an ability to manage change through proven, stable processes.
- Continual research into emerging risks and leading practices is part of the risk management program.
- Auditors are seen as an important component of risk management given their wealth of knowledge across the enterprise's programs and operations and expertise in internal control systems, fraud, waste and abuse, assessment and evaluation techniques, and root cause analysis.
- Action of audit finding does not languish on the back burner.

About the authors

Jeffrey C. Steinhoff

Managing Director, Federal Management Consulting
jsteinhoff@kpmg.com

Jeffrey C. Steinhoff is the managing director of the KPMG Government Institute and a managing director in KPMG's Federal Advisory practice. In 2008, he retired from GAO after a 40-year federal career, serving as Assistant Comptroller General of the United States for Accounting and Information Management and managing director for Financial Management and Assurance. He led GAO's largest audit unit, with responsibility for oversight of financial management and auditing issues across the federal government. Included were establishment of the Green Book and assessments of internal control under FMFIA and OMB Circular A-123. Jeff worked closely with Congress on the enactment of FMFIA, led GAO's oversight of FMFIA for 25 years, and testified before Congress and the SEC on internal controls. He is widely published and one of the authors of the 2008 Managing the Business Risk of Fraud: A Practical Guide, and the Fraud Risk Management Guide, published by COSO and the Association of Certified Fraud Examiners in 2016. Jeff is a fellow of the National Academy of Public Administration and a past national president of the 14,000 member Association of Government Accountants.

Laura A. Price

Partner, Advisory, Federal Risk Consulting
lprice@kpmg.com

Laura A. Price is a partner and Risk Consulting leader in KPMG's Federal Advisory practice. She not only assists federal agencies but also is involved in the development and leadership of KPMG's broader Risk Consulting practice. Laura currently serves clients in the Defense and Intelligence practices, and has worked across all sectors of the federal government as well as state and local government. Her responsibilities over almost 30 years include risk management and risk optimization; internal controls, including implementation of OMB Circular A-123 and the Green Book; information technology portfolio analysis and information protection; activity-based costing; alternatives analysis; forensic services; business-process improvement; and legal and regulatory compliance. Laura is also an executive fellow of the KPMG Government Institute. She coauthored, with Jeff, The KPMG Executive Guide to High-Performance in Federal Financial Management, as well as a number of white papers and professional journal articles. Included is "Navigating uncertainty through ERM – A practical approach to implementing OMB Circular A-123."

Edmund L. Green

Managing Director, Advisory, Internal Audit & Entrprse Risk
elgreen@kpmg.com

Edmund L. Green is a managing director in KPMG's Risk Consulting practice with over 30 years of cross-functional experience, including commercial and consumer credit, treasury operations, risk management, and internal controls, primarily with Fortune 500 financial services companies and federal, state, and local government agencies. His main focus at KPMG is on assisting clients with implementing or improving ERM programs and processes, with emphasis on governance, risk assessment, reporting and training. He has also assisted clients in the areas of third-party risk management, risk culture, and incentive compensation risk assessment. He holds an Executive Masters from the University of Pennsylvania, School of Engineering & Applied Sciences and the Wharton School as well as an MBA in Finance and BS in Accounting from LaSalle University. He is a Certified Public Accountant and a Certified Treasury Professional. Edmund is a frequent presenter and author and an executive fellow of the KPMG Government Institute.

About AFERM and the KPMG Government Institute

About AFERM

The purpose of the Association is to be a professional organization dedicated to the advancement of federal Enterprise Risk Management (ERM). The Association shall serve its members by providing a forum for discussion of issues relevant to participants in the federal risk management profession, sponsoring appropriate educational programs, encouraging professional development, influencing governmental risk management policies and practices, and serving as an advocate for the profession. The Association serves government officials and the public by sponsoring efforts to ensure full and fair accountability for management of risk in achieving organizational objectives.

www.aferm.org/

About the KPMG Government Institute

The KPMG Government Institute was established to serve as a strategic resource for government at all levels, and also for higher education and nonprofit entities seeking to achieve high standards of accountability, transparency, and performance. The Institute is a forum for ideas, a place to share leading practices, and a source of thought leadership to help governments address difficult challenges, such as effective and efficient program, operational and risk management, adherence to regulatory requirements, and fully leveraging technology.

Jeffrey C. Steinhoff
Managing Director, Government Institute
T: 703-286-8710
E: jsteinhoff@kpmg.com

www.kpmg.com/us/governmentinstitute

KPMG

Contact us

Laura A. Price
Partner, Risk Consulting Leader,
Federal Advisory
T: 703-286-8460
E: lprice@kpmg.com

Timothy J. Comello
Partner, Risk Consulting, Federal Advisory
T: 703-286-8580
E: tcomello@kpmg.com

Edmund L. Green
Managing Director, Risk Consulting,
and Member of KPMG's National ERM
Leadership Team
T: 703-286-8692
E: elgreen@kpmg.com

Jeffrey C. Steinhoff
Managing Director, Government Institute
T: 703-286-8710
E: jsteinhoff@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.