Strengthening Risk Management Before the Next Big Crisis

A SIX-STEP GUIDE

BY MARK BEASLEY, AL CHEN, AND ERICKA F. KRANITZ

As we begin to emerge from the pandemic, most business leaders, including those at the helm of state and local governments, are seeking ways to learn from this experience and to strengthen their level of preparedness for the next risk management crisis. In fact, our recent research finds that a strong majority of organizations (73 percent) report that there will be significant changes in their approach to continuity planning and crisis management processes.[1] These levels are even higher for state and local governments and nonprofits (84 percent of those surveyed). Some organizations are realizing that their approach to managing risks is woefully lacking in robustness and maturity.

Each year, through the work of the Enterprise Risk Management (ERM) Initiative at North Carolina State University, we work closely with business leaders across all sectors, including state and local governments, helping them identify opportunities to enhance their processes for getting their arms around the ever-changing risk landscape.[2] During the COVID-19 experience, we have provided hands-on coaching for government leaders and other executives about effective tactics and emerging best practices related to risk management processes. This included a municipality with a population of 500,000 and a $215 million budget, along with a larger municipality that has a population of more than one million people and an operating budget exceeding $1.5 billion. ERM has also advised two large state agencies.

Building on the reality that managing risks will remain challenging for all organizations, this article includes insights from our ongoing work to formulate a six-step guide. State and local government leaders can use this guide to refresh their organization's risk oversight capabilities to be ready for the inevitable next crisis, before it happens.

It's not getting easier

State and local government leaders have had a front-row seat in navigating the extraordinary events of the past year. They are still called upon to help manage many responses to risks triggered by the ongoing pandemic situation, including oversight of COVID-19 testing and vaccine distribution efforts, issuance of evolving social distancing community guidelines and policies, and responding to increased demands for existing services while managing a host of other issues related to social unrest, public safety, homelessness, cyber threats, political elections, and so on. At the same time, government leaders have had to address risks affecting core operations that have been disrupted, and as they anticipate what's next.

Leaders are looking for ways to better anticipate risks, especially as senior executives are being asked to provide more information about risks affecting their organizations. They are looking for new ways to elevate their organization's approach to navigating the ever-emerging risk landscape. Organizational leaders are convinced that complex and interrelated risks will continue

to emerge—and stakeholder expectations for more effective risk oversight will continue to grow.

Many leaders are embracing a more enterprise-wide approach to risk management that is centered on better anticipating risks that may emerge and affect what is strategically important. But many leaders are unsure of what steps they should take. Our objective in this article is to highlight how state and local government leaders can either jumpstart or strengthen their enterprise-wide risk management efforts to obtain strategic value. See the sidebar for a more detailed description of ERM.

Keep things simple: Use a frame of reference

Organizations can keep things simple by using a six-step framework to evaluate and enhance the enterprise-wide risk management processes. Because the concept of ERM isn't new, leaders have varying levels of understanding (and misunderstanding) about ERM's role and key elements. Therefore, the concept needs to be defined at the outset to make sure everyone is on the same page about ways in which ERM might be helpful and what comprises an effective risk management process. This has generally been accomplished through a brief overview at an existing meeting of the executive team. Keeping the process relatively simple and aligned with current business practices is generally a successful strategy. There will always be opportunities to enhance and make further improvements over time.

The approach we tend to use is linked to six key elements of an effective ERM process, which are illustrated in Exhibit 1. Its circular nature highlights the fact that ERM is intended to be a continual, ongoing process, since risks will never stop emerging. The five inset ovals highlight critical components that business leaders should take to launch an ERM process that can provide proactive risk insights for strategic decision-making. These five elements are influenced by the organization's culture and leadership, which sit at the center, emphasizing the importance of setting the tone at the top. These elements are also in line with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management framework issued in June 2017.[3] Let's briefly walk through the six steps that directly correspond to the six elements of an effective ERM process.

What Is ERM?

The goal of enterprise risk management (ERM) is to help organizational leaders identify and manage risks that could have a significant impact on the organization's ability to achieve its mission-critical strategic goals. In its simplest form, ERM is a way of thinking about current and emerging risks, as well as missed opportunities, so leaders can be better prepared to manage risks more nimbly and proactively and to creatively adapt to changing circumstances. Having an ongoing process and mindset that focuses on understanding and managing risks proactively helps make leaders better prepared and resilient, and better able to pivot and adapt to changing circumstances. The concept of ERM focuses on the entire organization, with the goal of providing a comprehensive, holistic, top-down view of risks when they emerge. It helps make risks visible across functional areas and allows leaders to see their inter-relationships.

EXHIBIT 1 | SIX ELEMENTS OF AN ERM PROCESS

84% of state and local governments report that there will be significant changes in their approach to continuity planning and crisis management processes.[1]

STEP 1

Start with a strategic lens

The goal of ERM is to help management better anticipate risks that might emerge, impeding the government's ability to provide mission-critical products and services. The key is to get individuals focused on what's most important—that is, make sure everyone has a clear understanding of what the government works at every day to fulfill its core mission. We like to refer to these as the entity's "crown jewels." So, an effective ERM process starts with Step 1, which is highlighted by the top oval labeled "Core Value Drivers and Strategy" in the ERM cycle shown in Exhibit 1.

Most state and local governments provide a multitude of services such as public safety, parks and recreation, education, healthcare and childcare services, and libraries. We begin by engaging in conversations with government leaders to ensure there is a consistent and clear understanding of what is strategically most critical to the organization's mission and strategic success. These conversations are often conducted in a management meeting or an educational training session or workshop to ensure that key leaders agree about what is most important to the entity's strategic success. Leaders from throughout the organization need to be included. A successful restart after COVID-19 needs enterprise-wide input from Human Resources, Finance, Budget and Planning, Information Technology, and core operational units including Waste Management, Public Safety, and Transportation, because the focus will be on anticipating risks that could have a significant strategic impact on the entire organization, not just an individual function or unit.

Developing a strategic lens should occur before considering risks that might impact the ability to be successful. Without consensus about what is strategically most important, management may be going in competing directions about what risks are of the highest priority for the state or local government to manage.

STEP 2

Use a strategic lens to identify risks

With a strong strategic point of focus, management is in a position to begin identifying risks that might affect the government's ability to deliver those mission-critical services or new strategic initiatives (as shown by the "Risk Identification" oval in Exhibit 1). It's helpful to start by asking two important questions about these mission-critical services:

1. What has to go right to deliver these services?
2. What assumptions are we making about our organization's ability to provide these services?

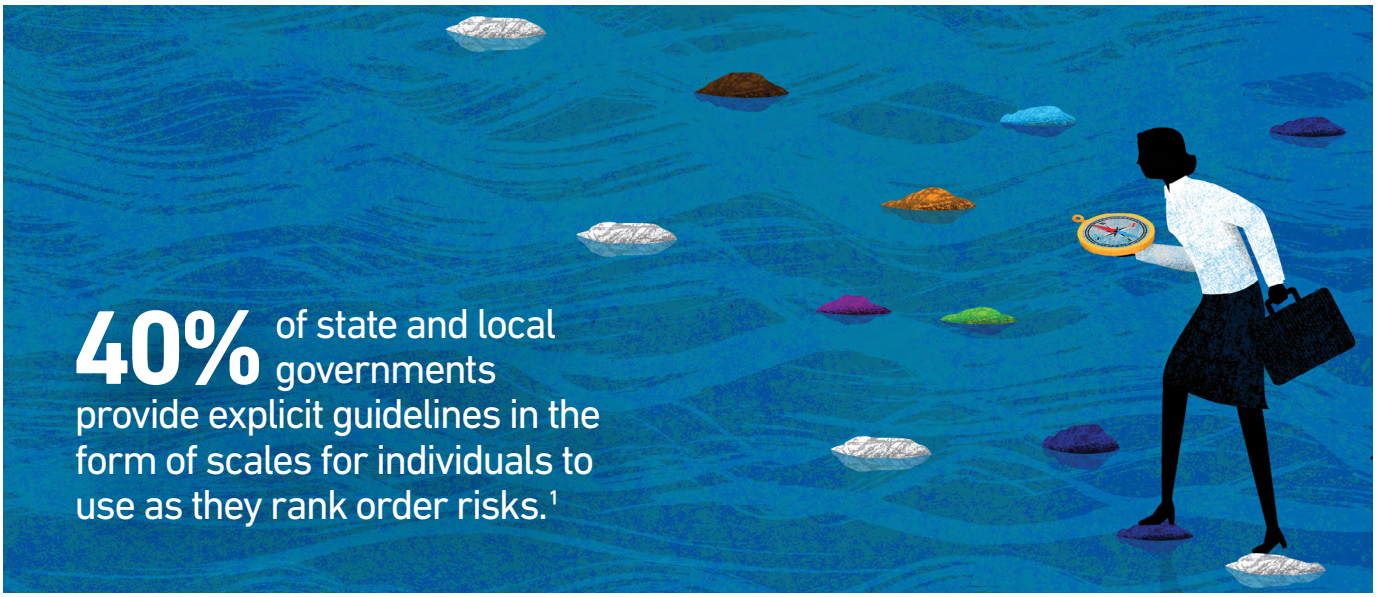
Once management thinks about these key elements, we then flip the first question to "What might emerge from within or external to the organization that might keep these from going right?" Answers to this question provide insights about potential risks on the horizon that are important to executing the government's mission-critical deliverables. Internal (from within the governmental entity) and external events (outside the control of the governmental entity) that might derail a process are great candidates to consider for potential risks that could emerge and impact strategic success.

Similarly, once the assumptions are pinpointed about the state or local government's ability to continue delivering mission-critical services, we then ask, "How do we know these assumptions are valid?" and "What is the impact to our success if an assumption is flawed?" For example, will critical IT systems support the increased volume of online business and core activities for employees working remotely? Answers help to tease out strong candidates for potential risks to what is strategically important for the state or local government to achieve.

Exhibit 2 provides a simple illustration of how these questions might help identify potential risks that might impact a local government's ability to secure books and database resources for libraries that serve their local community.

EXHIBIT 2 | RISK IDENTIFICATION TEMPLATE

MISSION-CRITICAL SERVICE	KEYS TO SUCCESS OF DRIVER What must go right for value driver to be successful? (Key people, processes, technologies, etc.)	BIG ASSUMPTIONS What are the big assumptions being made?
Example: Local library staff select books and databases for acquisition	▪ Librarians need to be knowledgeable about appropriate books and databases. ▪ The process of prioritizing books and databases for purchase needs to be accurate and reliable. ▪ The system for entering books and databases for purchase needs to be accurate and reliable and secure.	▪ Library staff is culturally competent to make selections that the community needs and desires. ▪ IT infrastructure can support the databases selected. ▪ The community can access the books and databases they desire.
POTENTIAL RISKS TO MISSION-CRITICAL SERVICE	**RISKS TO KEYS TO SUCCESS OF DRIVER** What challenges might emerge to prevent "keys to success"?	**RISKS TRIGGERED BY ASSUMPTIONS** What might challenge our assumption in the future?
	▪ Turnover in library staff may lead to deterioration of institutional knowledge. ▪ Management overrides process, leading to biased decisions. ▪ Systems used to select books and databases may crash or be inaccurate.	▪ Shifting community demographics may be overlooked when making book selections. ▪ Databases selected may not be compatible with entity's legacy IT systems.



STEP 3 Prioritize top risks

Most state and local governments face a plethora of risks, so a number of potential issues are identified in this step. Management needs a process to help them assess which risks are most important (as reflected by the "Risk Assessment" oval in Exhibit 1). A common approach is to rank risks based on impact, likelihood, preparedness, and velocity. A five-point scale numbered from 1 (low) to 5 (high) could be used to assess these elements of a given risk:

- **Impact** refers to how big an effect the risk would have on the organization, such as from a financial perspective or in terms of reputational damage.

  Example: The pandemic could have a negative economic impact on income tax revenues of more than 50 percent. (This would be considered high impact.)

- **Likelihood**, or probability, considers the chance of the risk occurring in a given period of time, usually two to three years.

  Example: There is a high probability that actual tax revenues will decrease by 25 percent or more than the amounts budgeted over the next fiscal year. (This would be considered a high likelihood.)

- **Preparedness** reflects whether the organization believes it has steps in place to manage the risk, should it occur.

  Example: Fund balance reserves and budget cuts will only sustain the current level of activity through the next fiscal year. (This would be a low level of preparedness.)

- **Velocity** considers the speed of onset, or how fast the risk might emerge. This element needs to be considered along with all other factors—for example, a risk may be determined unlikely, but it might evolve quickly and have a high impact if it appears. So, risk responses would need to be in place for trends that are fast-moving with disruptive potential.

  Example: The pandemic's onset has been fast-moving, with little advance warning about the potential extent and damage to business operations. (This would be considered high velocity.)

Risk scores can be developed from the assessments of each risk to rank-order risks from highest to lowest to pinpoint which risks deserve the most attention. The COVID pandemic prompted many state and local government leaders to realize that they must understand their top risks in order to effectively focus their limited resources on what is most important strategically to the organization overall.

Our *2021 State of Risk Oversight Report* finds that about 40 percent of state and local governments and nonprofit organizations provide explicit guidelines in the form of scales for individuals to use as they rank order risks. Those that do not provide these kinds of scales (or templates) sometimes just simply ask individual leaders to submit their ranking of top 10 risks from the list of risks identified in Step 2. The rankings from individuals can be aggregated to quickly pinpoint a consensus view of top risk concerns.

STEP 4

Develop risk response

Many risks are interrelated, so it's a good idea to assign a "risk owner" for each risk theme to keep management informed about top risks and communicate with a high-level internal risk committee. Risk owners help management keep an eye on all aspects of their assigned risks.

The risk owner is usually the person who leads a business function most closely related to the risk theme. For example, the vice president of Human Resources would likely be the risk owner for risks related to attracting and retaining key talent. Each risk owner is a "champion" responsible for developing a deep understanding of a group of related risks, identifying root causes. They will evaluate responses to prevent and/or manage the risk and monitor the risks for changes, both positive and negative. The risk owner is responsible for overseeing the organization's approach to managing a particular risk theme, such as talent, and identifying a team of subject matter experts to help address the organization's responses to the underlying individual risk statements.

The risk owner oversees the process to determine if the organization's current risk management approach adequately addresses each of the top risks and, if not, what additional responses or adjustments are necessary (as shown by the oval "Risk Response" in Exhibit 1). The goal is to consider how the organization is already managing the risk by taking steps to reduce the likelihood of its occurrence. This is achieved by understanding the root causes of the risk and finding ways to prevent those root causes from emerging. Risk owners also need to assess how prepared the organization is to manage the impact or consequences of a risk event. They also need to engage other subject matter experts who have direct responsibility for the activity or area related to the particular risk statement. Therefore, the risk owner, in conjunction with other members of management, would also determine what additional measures, if any, the organization needs to implement to enhance the effectiveness of its risk management.

A useful tool, referred to as a bow-tie analysis, helps in evaluating the root cause and the effectiveness of risk responses. Exhibit 3 provides an example of a completed bow-tie analysis.

Let's walk through an example of how a risk owner could use the bow-tie format to analyze an individual risk statement. The hypothetical risk is related to an outdated information technology system that can no longer support the government's current environment (see Exhibit 3). The risk is in the center of the bow-tie—it is the "knot."

A bow-tie analysis begins with a focus on possible root causes (which are illustrated in the far-left column of Exhibit 3). In this example, the unprecedented level of unemployment claims may be stretching the IT system capabilities. Also, employees who are working remotely may unintentionally create IT system vulnerabilities because of a lack of awareness and insufficient training. Many governments have older IT systems, and the capabilities of these systems, along with the IT support team, may not be able to keep ahead of the emerging cyber threats.

Next, the risk owner summarizes the measures currently in place to prevent these risks (see the second column from the left in the bow-tie analysis in Exhibit 3). Examples include cross-training employees and hiring part-time workers to keep up with the increased volume of claims. Organizations can also address cyber risks by conducting annual training and using third-party software to scan the network for unauthorized access attempts.

To the right of the center of the bow-tie analysis in Exhibit 3, the risk owner identifies consequences and responses for managing the risk event. For example, many state and local governments have already experienced a backlog of claims, given the increased volume and the time it takes to process unemployment benefits. A ransomware attack on a government's IT systems could make it difficult or impossible to provide core business processes for a period of time. Both of the above examples could also have a negative impact on the government's overall reputation. Possible actions for managing the impact of risk events may include eliminating non-value-added manual processes and evaluating a new IT system, or expanding its capacity, should these risks continue for a longer term.

A key ERM principle that has emerged during the past year is that risk owners must learn how to respond to risks quickly and effectively, without expecting perfection. The risk owner, in conjunction with other members of management, would also determine what additional measures the organization would need to implement in order to enhance the effectiveness of how they are managing the risk.

Risk owners must learn how to respond to risks quickly and effectively, without expecting perfection.

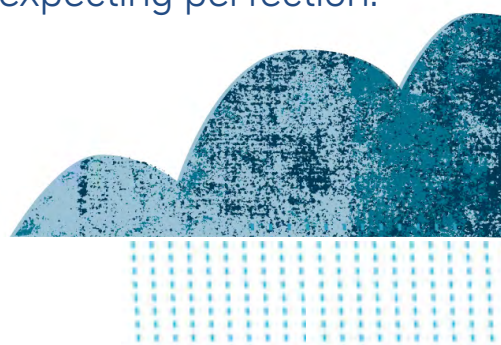


EXHIBIT 3 | BOW-TIE ANALYSIS TEMPLATE

CAUSES	RESPONSE TO PREVENT RISK	OWNER OF RESPONSE		CONSEQUENCES	RESPONSE TO MINIMIZE IMPACT	OWNER OF RESPONSE
▪ Significant increase in volume of unemployment claims in a short period of time. ▪ Current manual processes are inefficient and not designed for current situation.	▪ Cross-training of employees. ▪ Part-time employees hired for the near-term. ▪ Regular review of exception reports and metrics for unusual activities.	Individual #1	***The current information technology systems are outdated and may not be able to support the extent and nature of activities in the current environment.***	▪ Significant backlog of claims. ▪ Individuals unable to obtain status information. ▪ Negative impact to reputation and public image.	▪ Increase cross-training of employees. ▪ Reduce and/or eliminate manual processes considered low-risk. ▪ Evaluate long-term IT options, such as a new system or expanded server, to allow for increased volume and efficiency.	Individual #3
▪ Evolving cyber risks may outpace capabilities and knowledge of IT support especially due to employees working remotely. ▪ Improper data handling, storage, and/or disposal of information.	▪ Required annual training on best practices. ▪ Utilize a third party software to scan network.	Individual #2		▪ Various data systems attached by malware. ▪ Business interruption to core processes. ▪ Management may be unable to make reliable and/or timely business decisions due to inaccurate or incomplete data.	▪ Stronger access requirements (two factor) to key systems. ▪ Regular review of metrics and data analytics to support management decisions. ▪ Ongoing required education.	Individual #4

STEP 5

Communicate and monitor risks

To be truly effective, ERM should foster rich dialogue about the management of the top risks on the horizon that might derail mission-critical services. Effective communications about risks among the management team can help foster conversation that will help in making decisions. (This links to the "Communications" aspect of the last insert oval in Exhibit 1.)

A growing number of organizations are creating management-level risk committees to oversee and coordinate risk management efforts across the enterprise. Our *2021 State of Risk Oversight Report* reveals that 62 percent of organizations surveyed have a management-level committee in place in 2021, as compared to 22 percent over a decade ago. A management-level risk committee is an internal committee made up of senior leaders involved in strategic decisions throughout the entire organization. The committee's role is to evaluate and assess the effectiveness of the organization's response plans for specific risks. Communications from risk owners to risk committees help management engage in an open discussion as to whether the entity's risk response plans are reasonable and if leadership is comfortable with the level of residual risk accepted. The committee should meet regularly with the risk owners to review a summary about each of the assigned risks and the related risk responses.

Communication is essential to any organization, but even more so as the organization works through these ERM efforts. Many of these risk statements will be interrelated, so communications need to be transparent, and information should flow regularly throughout all levels of the organization and to the board or governing body.

Many entities are asking risk owners to prepare one-page risk templates that summarize all the key information related to a particular risk. (See Exhibit 4 for an example.) These templates are intentionally designed to be one-page summaries that provide a high-level overview for all members of the management team about a given risk. Of course, if more information is needed, the risk owners can be asked to provide it. Many organizations find these summaries very helpful.

Risk committees need metrics to help in their assessments (as indicated by "Monitoring" in the last oval in Exhibit 1). A lesson learned from dealing with COVID-19 and other events of the past year is that all types of entities must consistently monitor and communicate an organization's internal and external risks using key risk indicators (KRIs). Most organizations have several metrics, or key performance indicators, for monitoring historical activities. One example would be actual expenditures as compared to the appropriated and approved budget. These performance indicators (or KPIs) focus on the past and are usually based on internal data.

To identify KRIs that are relevant to each risk, think about the following questions.

- How would you know if one of your top risks was increasing?
- What would the warning signs be?
- Who is monitoring this?
- How would management be informed?
- What are the process and culture to support escalation?

EXHIBIT 4 | EXAMPLE OF A 1-PAGE RISK REPORT

Value Driver Theme: Talent Management

Tier 1 Risk Statement: There is a concern that we may struggle to attract and retain talent we need for strategic success.

Risk Owner: Jane Doe

High-Level Summary of the Risk Issue (i.e., what's happening, what are the root causes):

Job candidates and existing employees may no longer view our business and industry as interesting and attractive. Our compensation packages may not be sufficiently competitive to attract and retain needed talent.

What are We Doing Now to Prevent the Risk from Occurring (Preventive Response):	What are We Doing to Minimize Consequences of Risks If They Occur (Reactive Response):	Need for Additional Responses to Better Manage Risk Responses
Our website and other external communications in online hiring sites are emphasizing how our organization is innovative and dynamic and having an impact on our customers' lives. We have recently completed a compensation benchmarking analysis and have made market adjustments to key positions.	We have entered into a contract with a professional staffing agency to provide temporary staffing needed for key positions. Each key business function is cross-training individuals to ensure there is backup redundancy for key processes that must be operational.	We need to evaluate our existing benefits package to bring it up to date with expectations in the marketplace. We need to boost our work schedules to allow for more work-hour flexibility and work-from-home options.

How is this Risk Trending?
Increasing at a steady pace on a month-by-month basis.

How Fast Is this Risk Changing Over Time?
(i.e., what is its Speed of Onset)
Escalation of this risk may occur at a gradual and moderate pace (probably quarter over quarter versus oversight).

What Information Might Be Helpful in Monitoring this Risk?
(e.g., Key Risk Indicators):

- Turnover in key positions
- Percentage of employee complaints (or exit interviews) citing industry concerns or compensation/benefit concerns
- Trends in number of applications submitted for employment

When Would We Know that a Different Action Should be Taken?

- When turnover exceeds ____ positions in key roles
- Employee complaints begin to escalate to ____ percentage
- Key processes are interrupted and can't be completed on time.

What is Our Greatest Concern About this Risk?
If we can't reduce the risk of losing key talent and improve our recruiting efforts for new talent, the entity is likely to face delays in service deliveries that will lead to significant criticism and backlash from residents and other key stakeholders who are vocal in expressing their frustration in the media and other visible platforms.

STEP 6 Set the tone (culture and leadership)

The success of any significant initiative requires the right level of support at the highest levels of the organization, and ERM is no exception. The right tone at the top creates a culture that sees risk oversight as essential. This is why the entire larger oval in the ERM cycle diagram (in Exhibit 1) is shaded gray, indicating that culture and leadership are foundational to effective risk oversight. If the culture of an organization does not embrace the importance of risk management, then implementing an ERM process will not help.

It is vital to establish an environment in which individuals feel comfortable bringing concerns to management's attention. An organization can't effectively respond to risks if it doesn't know they exist. Leadership should communicate throughout the organization the importance of anticipating and managing risks that could derail the organization's strategic efforts. And leadership should ensure that the organization's culture has a positive impact on its risk oversight efforts.

The right tone at the top creates a culture that sees risk oversight as essential.

The time is now

Given the events of the past year, many organizations have had to quickly pivot to break down silos and build trust as leaders work together to maintain stability of the business and to manage the risks to the current business model. Many organizations are taking the time now to evaluate what worked and what did not over the past year and to learn from their experiences to determine the gaps in their ERM practices.

While ERM would not have prevented events like COVID-19 from affecting state and local governments, it can improve the preparedness and agility of government management teams in navigating risks that could have an enterprise-wide impact—like those caused by the pandemic. Government leaders realize that they need to move away from siloed thinking and instead work together to identify and manage those risks, as well as potential opportunities. ERM should help leaders work together to become more resilient and forward-thinking.

Mark Beasley *is a professor of accounting and director of the ERM Initiative at the Poole College of Management, North Carolina State University.* ***Al Chen*** *is a professor of accounting, graduate faculty, Department of Accounting, at the Poole College of Management.* ***Ericka F. Kranitz*** *is a lecturer in the Department of Accounting in the Poole College of Management.*

Beasley, Chen, and Kranitz serve in leadership positions within the Enterprise Risk Management (ERM) Initiative at NC State University (erm.ncsu.edu). The ERM Initiative provides thought leadership about ERM practices and their integration with strategy and corporate governance. Faculty in the ERM Initiative frequently work with boards of directors and senior management teams, helping them link ERM to strategy and governance.

NOTES

[1] 2021 State of Risk Oversight: An Overview of Enterprise Risk Management Practices, April 2021.

[2] The ERM Initiative is a thought leader advancing enterprise risk management practices, with an emphasis on the integration of ERM with strategic planning and governance (erm.ncsu.edu).

[3] See Enterprise Risk Management: Integrating with Strategy and Performance, COSO, 2017.