WHITE PAPER

EXPLOITING TECHNOLOGY FOR ENTERPRISE RISK MANAGEMENT IN THE PUBLIC SECTOR

THE CASE FOR ERM TECHNOLOGY
Since the revision of OMB Circular No. A-123, Management’s Responsibility for Enterprise Risk Management and Internal Control, in 2016, one thing enterprise risk management (ERM) teams in the public sector have learned is that ERM is no small undertaking. Documenting and understanding mission and objectives, risks to mission and objectives, fraud risks, outsourced risks, controls, control assurance and testing, and reporting is an overwhelming amount of work. The problem is compounded by the fact little, if any, of the ERM domain is static. Objectives, risks and controls change all the time. Some changes accompany changes within the organization, staff and technologies, while many others are associated with third-party service organizations or result from changes in vulnerabilities and external threats. Many changes cannot be easily anticipated, yet agencies are charged to effectively respond with alacrity when surprises arise.

Government organizations today face a rapidly changing regulatory and agency risk landscape and will likely continue to do so in the years to come. Their ERM strategy may not be positioned to adapt to these changes. Decentralized organizational structures, multiple tools, and various processes and systems make it difficult to see a clear and consistent risk picture across the organization. Additionally, the number, complexity and velocity of risks are increasing, and the speed at which these risks emerge means organizations have less time to effectively respond.

The recent global healthcare crisis provides an illustration of how an environmental risk can significantly impact the processes and functions a government organization is charged with providing. Agencies initially struggled to provide the services other dependent organizations and the general public rely on and require, and to ensure employee safety at the same time. The well-documented cyber breach at the U.S. Office of Personnel Management in 2015, with its corresponding identity risk and financial cost ramifications, provides another illustration of the unfortunate consequences of unanticipated and unaddressed risk.

Most risk management teams are managing different types of risk—cyber, third-party, personal, financial, policy, safety, environmental, public service and others, all typically in different silos—and assessing them using separate methodologies and measurements. Such an ad hoc risk management approach is likely overloading resources and isn’t providing a consistent, real-time, aggregated view of risk across the business to leadership teams. Without this visibility, risk cannot be consistently managed within the organization’s risk appetite.

Organizations are finding that existing risk and audit approaches, process, expertise and tools are not sufficient to deal with a dynamic and ever-evolving risk landscape. In addition, fewer resources and added responsibilities within risk and audit teams argue in favor of an approach that is more flexible, adaptive and transformational. Dynamic risk planning should be incorporated into approaches and results, driving risk and audit organizations to work more closely together. The executive team needs assurance that the organization’s internal control framework is adequately designed and operating to ensure that risk is being effectively managed, so that agency leaders have the confidence and complete understanding of the organization’s risk profile they need to make sound, risk-based decisions.
OPERATIONALIZING ERM

Effective ERM is synonymous with good governance, but good governance cannot be achieved without "operationalizing" ERM. Operationalization is necessary because enterprise risk is dynamic and quite voluminous, requiring the engagement of too many stakeholders to be done with available resources. Consider the method most organizations employ to capture objectives, risks and controls. Most organizations start out creating custom campaigns with Microsoft Excel templates that they mail to dozens or more managers, asking them to fill in the blanks—even while realizing that a good number of the managers will interpret the request in different ways, won’t be familiar with the terminology being used, and may not know how to assess a risk or write an internal control statement. Worst-case scenario, many managers will not respond on time, if at all. As a result, risk teams are caught up in an endless cycle of looking for response gaps and vetting the adequacy of responses received.

With risk management technology today, there is no reason to commit valuable resources to chasing down responses from managers. Here are examples of how integrated risk management solutions can operationalize ERM, saving resources and money, improving completeness and accuracy, and enhancing governance.

1. Automated workflow can distribute objectives, risks and controls collected in the last cycle to the current owners for rewording (if appropriate), reaffirmation and reassessment. If there are no records for a manager to review, a blank form can be distributed for managers to declare their objectives, processes, supporting objectives, key risks and key risk-mitigating controls. Terminology and assessment techniques can be explained with embedded help text, and blank fields can be minimized by requiring all fields be completed before the record can be submitted.

The risk management team has real-time graphic visibility into the status of management’s response: How far, from 1-100%, are managers from being complete? Risk teams can proactively reach out to managers that seem to be struggling. Workflow can send management reminders and automatically escalate past-due responses up the management chain. Risk teams no longer need to send and resend emails imploring managers to participate.

2. ERM technology today can be structured to capture information for regular refreshes of risk and control registers and risk assessments. Most ERM teams today endeavor to have management do these refreshes on at least an annual basis. Some publicly traded private sector organizations even expect them to be done on a quarterly basis! ERM technology today can also be structured not just to capture these refreshes but also to report all new and changed objectives, risks and controls, and associated risk assessments, to the ERM team for review and approval before being updated to the system of record. As a result, ERM teams no longer must look at every response but only those that change, and they play the pivotal role to make sure anything that goes into the system of record makes sense and conforms to
approved taxonomy, sentence conventions and assessment approaches.
Continuous monitoring of changes coming in from management across the
organization gives the ERM team near real-time visibility into changes in the
organization's risk profile. They may choose to engage in helping managers
with their new risk profile or simply report significant changes up to the
organization's governance teams.

3. ERM technology can help with the increasing challenges outsourced
services pose to organizations. Third-party risk is often opaque, and risk
assessments require the engagement of many stakeholders (legal, insurance
risk transfer, information security, compliance and business resiliency). With
an ever-increasing government dependency on third-party contractors and
technology organizations (and consequently, an expanded risk “footprint”),
an integrated risk management technology today can standardize the
process of collecting the inventory of third parties, documenting who “owns”
the relationship, and understanding the purpose of the relationship and how
significant it is to the organization. Automated workflow can be utilized to
solicit internal control questionnaires from third parties, and assess legal
contracts, insurance certificates and risk assessments. Go/no-go decisions
can be programmatically enforced consistent with the organization's risk
appetite and tolerance.

4. Reporting is dramatically simplified using integrated risk management
technology. Managers granted access can see an online, real-time profile
of risk within their domain of responsibility. Control gaps identified
through assertions, or management or audit testing, can automatically
open issues that are tracked from origination to disposition within the
accountable management chain. Periodic reporting, regardless of the cycle
(weekly, monthly, quarterly, etc.) is easily produced, including top risks,
key controls, objectives most at risk, vendors to watch, risk profile of most
important vendors, outstanding issues by criticality and due date, new
policies and policies to be reaffirmed, and policy exceptions and exceptions
to be reaffirmed.

These are just a few examples of possible ways ERM technology can be exploited
to save management and ERM teams time and money while improving the
organization's ERM capabilities.
EVALUATING ERM TECHNOLOGY

There are several factors risk managers should consider when evaluating ERM technology options.

USER INTERFACE (U.I.)

To maximize its usefulness, ERM technology must be accessible to and usable by each of the three lines of defense: line management, risk and compliance management, and independent audit. The U.I. should be modern, familiar and intuitive. Poor U.I.s will put off users and will result in lower usage. The U.I. of ERM technology should, to the extent possible, encourage participation and engagement.

STAKEHOLDER ENGAGEMENT

Beyond the user interface, ERM technology engages users in several ways.

- Configurable workflow can be used to automatically route problems, risk decisions, incidents, risk assessments and day-to-day risk management activities to accountable stakeholders.
- Workflow typically engages stakeholders via instant messaging and email. It is desirable to make certain that ERM technology can engage stakeholders regardless of the organization's messaging and mail solutions and that it can do so whether stakeholders are fixed at their workstations or are mobile.
- Modern ERM technology liberally utilizes due dates, ticklers and exception flags to escalate matters requiring management attention. For example, managers receive automatic notification when subordinates' commitments approach or exceed due dates; analysts receive notifications when documents are about to expire and need to be updated; and when continuous monitoring metrics fall outside acceptable boundaries or a risk level increases, stakeholders can be notified to act to remedy the problem. These features are important for any kind of risk management but are particularly important during information security incidents or business interruptions. When incidents and interruptions occur, it’s vital to have multiple individuals notified and working to minimize the event. Modern ERM technology is designed to optimize the handling of crises such as these and for senior management to know the real-time status via online dashboards.

CAPABILITY TO INTEGRATE

Many kinds of risk assessment require data input, and virtually all continuous monitoring requires data input related to the performance of controls. Consequently, it is critical that ERM technology can easily integrate external data. Some integration may be achieved with simple Microsoft Excel or CSV file uploads. Other cases may warrant online, real-time integrations that require no human involvement. ERM technology integration should be carefully evaluated in terms of flexible integration architectures, long-term project objectives and the kinds of data to be integrated.

When incidents and interruptions occur, it’s vital to have multiple individuals notified and working to minimize the event.
CONFIGURABLE CALCULATIONS

Risk assessments, control evaluations and exception handling all require calculations. In some cases, these may be as simple as arithmetic operations and conditional if-then-else statements based on numerical variables. In other cases, they may call for sophisticated equations and stochastic modeling of large and volatile risks. ERM technology should be able to accommodate all kinds of calculations without using complicated, esoteric coding.

REPORTING

It is critically important that ERM technology be able to produce the wide array of reporting required by each stakeholder and that the reporting engine be sufficiently flexible to allow the creation of new reports without utilizing traditional programming. Before acquiring any ERM technology, risk managers should survey key stakeholders to find out what kind of risk management reports they would like to have. The compiled list can then be used to methodically assess ERM technologies’ reporting capability. If the organization is already settled on a third-party reporting package (such as Tableau), the ERM technology will need to adequately interface with those technologies, too.

OTHER CONSIDERATIONS

The ownership of ERM-related technology solutions tends to vary by organization based on the size and maturity of the risk management teams and their experience with risk management principles and operations. It is not uncommon for Internal Audit functions initially to take responsibility for ERM systems because auditors often have the most experience in the evaluation of people, processes and technologies, and they are familiar with effectively structuring internal control frameworks. From this perspective, it makes sense for auditors to administer ERM technology, provided they can maintain independence. At a minimum, this means formally acknowledging that they do not “own” the internal control framework; the rest of the organization does. Maintaining independence when auditors are tasked with administering ERM technology may mean that all records documented in an ERM system are explicitly owned by named individuals outside of the audit function and that all changes to records in the ERM system are reviewed and approved by outside individuals.

As organizations mature and expand their risk management functions, ERM system administration can be distributed to a second line of defense function and internal auditors can return exclusively to a third line of defense role, independently evaluating the design and effectiveness of management’s internal controls.
Regardless of where an organization decides to place ERM system administration, the benefits to Internal Audit will be indisputable. In the absence of ERM technology, internal auditors are required to interview various levels of management and staff just to understand and plan the scope of an audit, as well as the risks and controls to be evaluated within the planned audit. Imagine a management system where all the needed planning inputs already reside: strategies, supporting processes, third-party dependencies, supporting physical and technology assets, risks, controls, policies, standards, prior and existing issues, losses and incidents. With this amount of detail, the creation of audit plans and workpapers can be populated automatically, if the ERM technology specifically incorporates integrated audit planning, workpaper creation, documentation and testing.

The ease of implementing ERM technology should not be oversold. Depending on the maturity and resources of an organization, implementation can be challenging. Organizations that have not addressed foundational ERM policies and practices should devote time to that before considering technology. For the rest, ERM system implementation can be broken up into manageable pieces, focusing first on the most pressing concerns of the organization. Each piece that is implemented fits together with previously implemented pieces until a holistic ERM system emerges.

**POSITIVE OUTCOMES OF ERM TECHNOLOGY**

Risk managers should expect to realize the following positive outcomes from deploying ERM technology that has been carefully selected to meet the organization’s needs.

**VISIBILITY AND BUSINESS CONTEXT**

Stakeholders will have more visibility into the organization’s risk and internal controls, and the risk and controls associated with outsourced services. Management will better understand what mission and objectives the risk and controls relate to. This visibility and context will make it easier for stakeholders to make consistent business decisions, including where scarce risk management resources should be allocated.

**LEADERSHIP ACCEPTANCE**

An ERM program that provides consistent and accurate results is likely to have more immediate leadership acceptance because the process is sound and historical results have demonstrated consistency.

**ORGANIZATIONWIDE IMPACT**

Enterprise adoption across all the organizational elements drives a consistent dialog in which everyone is speaking the same language and using a common taxonomy.
ACCOUNTABILITY
ERM technology establishes accountability by making it clear which named individual and business unit are responsible for an objective, business process, risk, control, policy or outstanding issue. Accountability leads to more timely and effective risk management.

CONSISTENCY
Consistency in risk assessments and decision workflow means risks will be handled in a consistent manner. There will be fewer exceptions in risk management because risk evaluation has been made consistent through operationalized assessments and decision workflow.

LOSSES AND INCIDENTS
Effective ERM programs are characterized by fewer surprises, losses and incidents. Losses are subject to methodical root cause analysis and remediation, and incidents are handled more quickly, so they are limited in duration and impact.

FINANCIAL IMPLICATIONS
A finely tuned ERM program can highlight possible cost issues on the horizon and drive action to avoid and even reduce anticipated costs based on recommended changes to processes.

TAKING THE ERM JOURNEY STEP BY STEP
ERM presents a formidable challenge for government organizations facing risk factors on multiple fronts including regulatory changes. Whether dealing with a cyber attack (as was the case at OPM), a national healthcare crisis, third-party breach, financial challenge, safety issue, environmental catastrophe or other risk event, an agency’s executive team and agency leadership must have confidence that they have a complete understanding of the organization’s risk profile and status in order to make good business decisions and fulfill their fiduciary obligation. They need assurance that the organization’s internal control framework is adequately designed and operating to ensure that risk is understood and effectively managed.

Developing, building, evolving and leveraging an organizationwide ERM capability is a journey and takes real commitment. Many agencies are on the journey, and while some are further along than others, most are still putting in place key pieces and processes to build upon. Having a solid ERM foundation leveraging a modern risk management technology that can support an organization on its journey is key to a fully developed, optimized and successful ERM program. With a sound, informed approach to evaluating technology for this purpose, risk managers can expect to realize a variety of positive outcomes from operationalizing ERM in their organizations.
RSA ARCHER® INTEGRATED RISK MANAGEMENT

With the RSA Archer Operational Risk Management use case for enterprise and operational risk management, organizations can harness risk intelligence, reducing the likelihood of negative events, lost opportunities and surprises. The use case is part of the RSA Archer Suite, which serves as a central aggregation, visualization and governance point, consolidating risk data from siloed risk repositories to make it possible to better understand, prioritize and manage risk, and reinforce risk management accountabilities and culture. Go online to learn more about RSA Archer Public Sector Solutions.

ABOUT RSA ARCHER SUITE

RSA Archer Suite enables organizations to manage the broad dimensions of risk and confidently pursue digital opportunity. The suite is part of the RSA portfolio of business-driven security solutions, which provides a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.