This whitepaper is the first in a series of four addressing the tactical implementation, and then holistic integration, of Enterprise Risk, Business Resiliency and Strategic Planning programs.

Operationalizing Risk Management

A Roadmap for Getting There

The Trouble with Risk Management

An organization seeking to establish its first true risk management program and/or mature its existing program into an enterprise risk management capability can find the process daunting. There is a myriad of frameworks, theories and best practice standards that vary based on industry, business model and public/private/non-profit sector. While the risk management process itself is (fairly) straightforward, what is not so clear is how to successfully operationalize the program in a way that creates synergy across the organization and positively impacts strategic objectives and resilience capability. The hurdles faced are not uncommon to the implementation of any kind of organizational program that requires systemic change, including technical competency and understanding of best practice, selection of appropriate framework (or frameworks), and ability to design effectively given the unique qualities of leadership, culture and operational maturity of the entity. Also important are determining the depth and breadth of the program desired, and consideration of how a new program implementation can be managed in a way that supports, rather than interferes, with existing strategic priorities, and that can be accomplished within finite resources.

When I first entered the world of risk management, I was incredibly frustrated at the lack of clarity within the voluminous materials, models and standards that existed. Being a typical corporate manager pressed with too much work and not enough resources, I was looking for an A-B-C manual that would allow me to plop a program into place and call it good. That was, of course, not possible and for good reason. I came to learn that along with the science, there is an art to designing, implementing and sustaining a true risk management program, and that a holistic understanding of organizational schema is required to build a program that integrates horizontally across functional silos and is appropriately applied at every tier of the organization. That was a bit of a mouthful, so let me jump to the end of the story and break it down with some lessons from the trenches:

> ***Lesson One: Organizations = People****. If you want to make real change, you must anticipate the impact that any modification of process/practice/methodology will have on people. If your risk manager is highly analytical, this point may be lost on them so its important they have input and guidance from those more in-tune with personnel and change management philosophy.*

Lesson Two: The program must functionally fit the the organization. *If a system, method or process is not operationally feasible within available resource, it will be rejected before it has time to proof its worth – it simply cannot be designed without consideration of the operation. Your Risk Manager, and I would argue no one, is equipped to tackle this alone, so please don't send them off to be Don Quixote jousting windmills within your organization.*

Lesson Three: Value drives sustainability. *This feels a bit obvious, but it's important enough to call out. Tangible value must be articulated for every process – people are more easily persuaded to adopt change when they perceive a personal value to following a new routine. It doesn't have to be big, sometimes just knowing that their participation in the process gives them air cover through more transparent decision processes is all that's needed.*

Lesson Four: Sustainability requires persistence. *Program designers must recognize and plan for staff turnover, complacency, and change in business practice. While implementation is the main hurdle, regular maintenance of the program is required. New employees must be trained, program KPIs (key performance measures) must be tracked and reported, and failsafe measures built-in for those ornery employees who just don't like to follow rules.*

So, if you haven't run away screaming at this point (ok…. maybe just tossed this in the trash) good for you! A lot to ask you say? Yes. Unmanageable you ask? No. Building and implementing a risk management program and enterprise risk competency is just like any other – meaningful direction from the top (a must), technical knowledge, and a project approach with clearly defined outcomes will set the stage for success. In short, like the proverbial "eating an elephant" we design for the future state and implement one bite at a time.

Risk Management Function vs. Enterprise Risk Management Discipline

Risk Management is simply the process of identification, measurement and treatment of risks to avoid or minimize negative impact. This is the most commonly understood definition of risk management, and encompasses specifically hazard losses such as injuries, property damage, lawsuits and other related exposures that are typically covered by insurance. From a functional perspective, traditional risk management focuses on safety programs, catastrophic environmental hazards, and priorities addressing environmental compliance relevant to organization's industry. A risk function may also incorporate management of the casualty insurance program in cooperation with the finance department (always best given the direct correlation of premiums to exposures such as injury costs, revenue, property values and payroll). It is important to note, however, that even though they are not labeled as such, risk management activities are going on all over the company: contract review and administration, liquidity and credit balancing, asset maintenance and upgrade, due diligence for mergers and acquisition, business case development for new product or service lines, board reviews, marketing and social media campaign reviews, and the list goes on. The primary point here is that no organization is devoid of risk management, it simply (if typical) is carried out in functional silos and at varying levels of formality throughout the organization. The challenge is determining if these disjointed processes are really capturing, measuring and reporting risk in a way that key decision-makers can respond to them appropriately and timely. The answer is different for every organization.

Beginning in the late 1990s, the concept of Enterprise Risk Management (ERM) started becoming part of the corporate vernacular in the wake of breathtaking mismanagement scandals that took down the likes of Enron, WorldCom and LTCM. Driven by shareholder demand for increased transparency and reporting, regulatory bodies responded with standards that required new expansive, documented governance processes including the Sarbanes-Oxley Act, New York Stock Exchange Rules, and Standard & Poor's Debt Rating revisions. Concurrently, the International Standards Organization (ISO), Committee of Sponsoring Organizations (COSO), and Risk & Insurance Management Society (RIMS) took the lead in putting pen to paper to begin formalizing a standardized, repeatable framework for risk identification and treatment with the intention of driving risk competencies to a more strategic level to improve decision making in the C-Suite. With an integrated risk/strategy program in mind, ERM is defined

ERM is defined as a strategic business discipline that allows an organization to manage risks and seize opportunities related to the achievement of its objectives.

as a strategic business discipline that allows an organization to manage risks and seize opportunities related to the achievement of its objectives. An ERM framework creates the foundation for risk and opportunity to be identified, analyzed and managed within an interrelated risk portfolio. In short, it puts consideration of risk (both positive and negative) front and center in every key decision making process within the organization. Now, while regulation forced these new changes on publicly traded companies, financial institutions, and others of similar ilk, there are many more companies and organizations that were not caught up in that net. Thus, the best practice frameworks created by RIMS, ISO and COSO were intended to support regulation for those who needed it, but also be applicable on a much broader basis. Best practice frameworks are intended to be guidelines, not absolutes, thus the conundrum faced when determining best fit for an organization. Even so, I would proffer that ERM represents best practice management competency for any organization, regardless of industry, sector or size.

So, if my prior statement is correct (and it is!) then when why is ERM such an elusive goal? Why do we see implementation primarily within organizations where regulation absolutely requires it? There are many reasons, but the following usually hit the top of the charts.

- **ERM programs are complicated and expensive.** Possibly…. but they don't have to be. Overbuilding a ERM program (or building it too quickly) is not only a waste of resources, but it will very likely fail because it cannot be easily followed or managed. And, when people become frustrated with a process, they will either find an end-around or it will be abandoned altogether. Intentionally defining purpose, objectives and key performance indicators is the only way to track both Return on Investment and Return on Value for a maturing ERM program.

- **ERM programs slow down the business.** This is sadly true in many cases – refer to issue number one above. Because identification and measurement of risk lends itself so easily to deep analytics, it is easy to build complex matrices and risk registers, madly compiling data until all have forgotten why its being done in the first place. A properly constructed ERM program integrates with other existing programs, practices and procedures, leveraging, enhancing and ultimately improving an organization's internal mechanisms over time, resulting in more effective and efficient management systems.

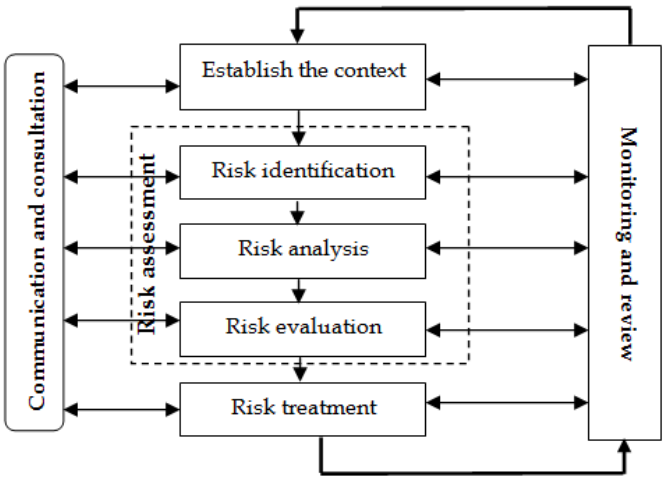
- **ERM is only for "the big guys".** Nope, but good try. The "big guys" got big because they understood how to capture and utilize risk information to formulate and drive strategy. The ones that have been around for a while understood also that a successful organization requires identification of emerging risk and opportunities, nimble operations, and internal resiliency. *Regardless of size, industry or even profit/non-profit sector, sound management practice requires that the right people have the right information at the right time to make the best possible decision. This is the essence of ERM discipline!* And while there are specific characteristics that are common to all ERM programs, the size, shape, color and personality of any one program is not fixed and should not be presumed.

So, let's recap. ERM is a strategic business discipline that allows an organization to manage risks and seize opportunities related to the achievement of its objectives. To accomplish this, standardized, repeatable processes must exist to allow relevant information to flow up and across the organization in a timely manner. As much as its strategy, ERM is unique to every entity and must be designed using best practice (and sometimes a variety of them) to fit the distinctive organizational personality. Program elements must fit well and compliment existing process,

procedure and management structure. Finally, the outputs of ERM must be designed from the ground up and into strategy development, with program accountability based on key performance indicators relevant to the operation of the organization. Now that we've defined the big picture, let's drop back down to the fifty-foot level and talk about the foundational elements of a risk management program.

Risk Management & ERM – The Basics

In this section, I am going to walk through the essentials of risk management process, and I will discuss how each is then elevated to an ERM competency. The ISO 31000 Risk Management Process Framework provides the best illustration of this iterative cycle that serves as the foundation for most risk management practice, and thus it is intuitive to most management and leadership teams despite the likely use of different nomenclature. *Context* simply means that we must understand the scope and assumptions for what we are attempting to risk-manage, and *Identification* calls for a brainstorming of all possible risks within that scope. *Analysis* determines what the potential impact of an identified risk is to the organization in terms that are meaningful (loss of revenue for example), *Evaluation* determines where that risk exposure fits within the larger context of the entire organization, and then *Treatment* determines options for handling the exposure, as well as identifying any residual risk. As with any best practice, this process is iterative lending to the ongoing communication, monitoring, re-evaluation (and re-prioritization) of risks over time and as the business changes. I will briefly delve into each of these topics to point out some of the key success factors and pitfalls encountered when moving from theory to reality.



Context. Establishing the context is all about planning, and may well be the most overlooked and misunderstood component of risk management, either as a function or a discipline. Context for a risk management process means identifying the scope, goals, outcomes and resources required for thing (process, department, business venture, etc.) being evaluated. This is not unlike any other project where 'planning the work and working the plan' is the battle cry. As risks across an organization are fluid, so are the risk processes that are used – this is what gives flexibility to the program – but because *Context* defines the 6Ws[1] for the program, these variable processes are also complimentary. Now, context for ERM happens at a higher level, where an understanding of both internal and external forces at play within an organization (think Strengths, Weaknesses, Opportunities, Threats) is combined with strategic vision and objectives to define the organization's Risk Appetite and Capacity. With this knowledge, we begin crafting a program that targets mission critical elements of the organization, aligning time, energy and resource to the issues that matter most. Understanding Risk Capacity to define a clear Risk Appetite statement is not only foundation for ERM, but for strategic planning itself. Risk Appetite and Capacity statements ensure that strategy and risk are balanced, that objectives are properly prioritized, and set the tone for cascading management processes.

Risk Identification. Risk Management begins with the identification all sources of risk, areas of impacts, events and their causes and potential consequences to generate a comprehensive list for Risk Analysis and Evaluation (which is where the measuring comes in.) From a traditional functional perspective, this is generally equated with safety

[1] Who is responsible; What is the process; Why are we analyzing; When is the process triggered; How do we know its working; and Where do we report findings.

hazard evaluation of systems, processes and environments. From an ERM perspective, the focus is broader, and includes events that might create, enhance, prevent, degrade, accelerate or delay the achievement of strategic objectives, as well as assessing the risk of not pursuing opportunity. Risks not under the control of the organization are identified along with those that are, and include cumulative as well as cascading effects.

The types of risks an organization deals with can be categorized within four main buckets which may be expanded when relevant. Under this traditional model, risks are managed in a silo fashion, and risk management as a function focuses only on hazard loss with a directive to mitigate negative impact from those activities most commonly driving such losses. It is pertinent to note here that the functional responsibility for managing risk does not change with the implementation of an ERM discipline. Rather, ERM processes lay the foundation to systematically capture, measure and report risk within each functional area.

	Hazard	***Financial***	***Operational***	***Strategic***
Risk Scope	Employee injury Environmental spill Property damage Natural catastrophe Liability torts	Pricing risk Asset risk Currency risk Liquidity risk	Data security Data integrity Customer satisfaction Product failure Knowledge drain	Competition Social trend Capital availability, Competition Reputational risk
Traditional Responsibility	Risk/HSET	CFO	COO and Division / Functional Manager	CEO / C-Suite / Board
Traditional Risk Function	Claims Management Employee Safety Environmental Compliance/ Reporting Casualty Insurance Emergency Response	Accounting Controls Credit/Bond Facilities M&A Due Diligence	Specific to operational focus	Strategic Planning Key decision making

Recall that ERM is not a function, but a strategic business discipline. Division heads and operational subject matter experts (SMEs) are the best source for understanding and managing risk within their respective areas – ERM gives them a vehicle to communicate both problems and solutions in a common language that is easier to digest and respond to at an executive level. The role of the Risk Manager is to assist with the risk identification process, focusing on the capture of relevant data from SMEs. *Pitfall: ERM should not remove ownership of risk management responsibility from functional areas – risk managers own the process, not the risk.*

Risk Analysis. Risk analysis involves developing an understanding of the risk, including the sources, impact, likelihood and other relevant attributes. When we talk about traditional hazard loss risk, we are concerned with both Probability and Impact (or Severity). These measures can be quantitative, qualitative or a combination of both depending on the type of risk assessed as well as the program maturity of the organization. This analysis is generally underpinned by a calculation that determines Probability and Impact on an axis across various categories – for instance, an employee injury may impact operations (downtime & claim costs), reputation, and regulatory fines. Here we are looking to develop a systematic process for capturing and measuring potential impact of identified risks. This results in a common vocabulary that, in conjunction with guidance from Risk Appetite and Tolerance statements, allows for a timely and more measured conversation about risk to occur. Understand that a determination of "high risk" with no Context means everything and nothing all at the same time because every brain in the conversation will come to a different conclusion. *Pitfall: Overly complicated risk registers and calculations can easily derail the program.* Focus on Risk Tolerance guidance and build a process that is fit-for-purpose as well as appropriate for current organizational maturity. The first couple of years an entity may use all qualitative measures (high, medium, low) and then gradually begin incorporating more quantifiable elements. This is perfectly fine – as the discipline matures, the program and tools will naturally evolve on their own.

Risk Evaluation. As Risk Assessment identifies exposures and potential impacts, now Risk Evaluation looks specifically at how they play out within the organization with the specific purpose of determining which risks need treatment and the priority for treatment implementation. Take our example above regarding an employee injury; for the average company the impact may primarily be claim costs, but for a heavily regulated organization (think nuclear or remediation) that same injury could also spur high impact regulatory fines and adverse media affecting the organization's reputation. In this stage, we are acknowledging all risks, but weighting them by relevance for the

specific entity. Second, we look at risks from a consolidated perspective to identify those that show up in more than one area and/or that have the potential to increase impact across functional areas through a domino effect. Finally, we consider prioritization of risk by functional area, as well as for the whole entity. Since a high risk in one area may, in the grand scheme of things, be a low risk to the organization, or conversely something considered low risk may not be at all when its discovered that it exists across several functional areas, this exercise improves resource allocation in addressing "game-over" problems or simply low-hanging fruit as top priorities. ***Pitfall: Analysis paralysis.*** Many a program starts going sideways at this point and a couple of things generally happen. Small, every day risks are considered low risk (due to low impact) despite high frequency and desensitization obscures the fact that they are nickel-and-diming the company to death. Second, big hairy scary exposures are deemed low risk due to low probability, or are considered unmanageable and thus summarily dismissed. So here is where we point you back to the section on Context and Risk Tolerance because that will address much of this problem before it even starts (yes, you should go back and read it again right now). Then, we will continue with a quick side tour to discuss Control-Based ERM.

Risk Treatment. Once identified, traditional risk management calls for dealing with (or Treating) risk exposures in four ways, Avoidance, Reduction, Transfer or Acceptance. The choice of which to use is not always clear, and depends on an understanding of impact, cost and effectiveness. Once a determination is made on how an exposure will be treated, the anticipated effectiveness of that solution will be factored back in to the Risk Evaluation to determine the residual risk that remains and to calculate a new risk score. It should be noted that other than total Avoidance, no risk can be 100% mitigated, and some may require more than one technique or solution – consider a company mitigating construction project risk by i) Reduction through project size, ii) Transfer through subcontractor indemnity and bonding, and iii) Transfer through its own Builder's Risk Insurance program. ***Key Success Factor: Be creative!*** Many exposures are best tackled with a multi-faceted approach, and not every risk can or should be insured away.

Reduction: Organization takes action to reduce the likelihood or impact related to the risk

Risk Transfer: Risk is shared with others through insurance, contract indemnity and bond requirements

Avoidance: Organization exits the activities giving rise to risk

Acceptance: No action is taken due to low material impact or cost/benefit decision

Communication & Consultation. To make the risk identification, evaluation and treatment discussions relevant, operationally viable and realistic, subject matter experts across the organization must be engaged in the process for both consultation and validation (what we call gut-checking). As indicated earlier, the risk manager will become the program expert whose main mission is to assist operational SMEs with the process within the framework established by the entity, as well as to help identify when there is an information or input gap on more strategic due diligence projects. If it is not obvious at this point, successful ERM requires a willingness to create and maintain communication channels within the organization, and leaders will need to be mindful of spotting managers who block and hoard information from their teams rather than compile, synthesize and communicate it up the chain. ***Pitfall: Excluding Internal Risk Management from Due Diligence efforts.*** Every leader knows that their success comes from their team, and the concept of open communication to allow information to bubble up is nothing new. However, when strategic moves and opportunities are presented at the top, deep and holistic internal vetting is often overlooked. Opportunities are evaluated first and foremost on a risk/reward basis tied to return on investment, market expansion, revenue generation, etc. There is a lot of legal this and market analysis that with graphs and projections and computations galore. I am not dismissing any of that critical and relevant work. The gap I am talking about is typically in post phase – implementation / merger / acquisition – when suddenly your internal SMEs must quickly digest, adapt and manage this fabulous new thing. What happens when the product you launched is going like hotcakes but the sales team doesn't have the manpower keep up; or your repair team cannot troubleshoot the new piece of equipment customers are clamoring for because their test units aren't compatible; or the contract is inked for a near-belly up company (which you got a great deal on!) but then your surety suddenly terminates because your risk now exceeds their appetite? Sure, these things can usually be fixed, but it will be expensive and distracting.

Allowing your internal team in only after the "go" decision has been made is a bit like closing the barn door after the horses are off and running. In addition to the inefficiency, this oversight leaves your operational SMEs and Risk Manager feeling underutilized and their skills unappreciated; they begin losing confidence in the process and ERM begins sliding downhill. There are a multitude of ways to get the requisite operational input you need, yet still keep the secret squirrels secret, and its worth the extra effort on the front end to avoid post-go decision pitfalls.

Monitoring & Review. The final component of the ISO 31000 Risk Management Framework is monitoring and review. This is also a cyclical process that delivers continuous improvement within the program. As the business or environment changes, existing risk issues will be reviewed through the process and treatments changed or adjusted based on need. New issues will arise from the review of others, and occasionally fixes don't fix and need to be reimagined. Over time, the documentation collected will be invaluable because something magical happens when write stuff down. A division manager considering a vendor for a job can determine if they've had bad performance with the company some distant time in the past, training new staff at every level is easier and more efficient, and project stumbles can be assessed through lessons learned to be avoided in the future.

Hopefully, this brief primer has somewhat de-mystified the risk management process, and has illuminated the fact that risk management is already part of the fabric of your organization. Taking that capability and evolving it into a more standardized and formalized process that breaks across functional silos with guidance provided by the C-Suite (and Board if relevant) will move you into an ERM competency.

Enterprise Risk Management Best Practice

So how do you judge an organization's ERM maturity? There are a handful of models out there to gauge ERM capabilities, the most comprehensive of which is the RIMS Risk Maturity Model (RMM). Designed for broad use, RMM incorporates and maps to six different risk standards, including ISO and COSO, OGEC's Governance Risk and Compliance Model; it's this holistic approach that makes it so readily usable in almost any application. It identifies seven key attributes for effective ERM, covering the planning and governance of the program, as well as the execution of assessments, and aggregation and analysis of risk information. Each attribute includes a set of competency drivers which outline the key readiness indicators (or activities) involved in achieving each driver. These driver/indicator pairs cover the entire risk management process including administration, outreach, data collection and aggregation and analysis of risk information.

Now, before you think I'm selling something, the RMM is a free resource for risk practitioners and is good for looking specifically at ERM (Baldrige Excellence Criteria and other models are also very relevant and will be discussed in future white papers for their relevance to fully integrated risk, strategy and resilience functions.) I like to use RMM because RIMS has already done much of the legwork by compiling the various standards into its maturity framework, and using the assessment can help an entity determine at the outset what ERM areas need strengthening (or building), and allows leadership to visualize a future-state and set expectations for program outputs. ***Key Success Factor: Utilize this tool as a guide and not an imperative.*** First, while all attributes should eventually exist, the breadth and depth of each will vary depending on your organization. Second, as indicated by the name, this is a maturity model, and regardless of the method, maturity takes time. The reality of implementation within the typical resource-constrained operation will result in the prioritization of program elements to be developed. Ensure that your overall program design anticipates this measured approach, identifies key milestones, and defined success targets. This manages reasonable expectations in the C-Suite and Boardroom, as well as helps your go-to people maintain enthusiasm with tangible accomplishments.

Regardless of method, maturity takes time.

RMM Attributes

1. **Adoption of ERM-Based Process:** This attribute measures the organization's risk culture and considers the degree of executive and board-level support for enterprise risk management.
2. **ERM Process Management:** This attribute measures the extent to which the organization has adopted an ERM methodology throughout its culture and business decisions, and how well the risk management program follows best practice steps to identify, assess, evaluate, mitigate, and monitor risks.
3. **Risk Appetite Management:** This attribute evaluates the level of awareness around risk-reward trade-offs, accountability for risk, defining risk tolerances, and whether the organization is effective in closing the gap between potential and actual risk.
4. **Root Cause Discipline:** This attribute assesses the extent to which an organization identifies risk by source, or root cause, versus the symptoms and outcomes they produce.
5. **Uncovering Risks:** This attribute measures the quality and coverage of your risk assessments. It examines the method of collecting risk information, the risk assessment process and whether enterprise-wide trends and correlations can be uncovered from the risk information.
6. **Performance Management:** This attribute determines the degree to which an organization executes on its visions and strategy. It evaluates the strength in planning, communicating and measuring core enterprise goals with a risk-based process, and the extent to which progress deviates from expectations.
7. **Business Resiliency and Sustainability:** This attribute evaluates the extent to which business continuity, operational planning and other sustainability activities are approached with a risk-based methodology.

Seizing Opportunities – the Up-Side of ERM

The emphasis with ERM is that it is strategic, allowing us to manage risks AND seize opportunities, but negative risk and how to manage it has really dominated the discussion thus far, and too often is where the understanding ends. However, ERM is just as much about seizing opportunity as it is about managing risk. A natural byproduct of brain storming and then deep-diving on risk issues is the uncovering of opportunities that may balance those risks. A more intention process can be achieved by taking the framework above, and replacing the word risk with opportunity. I will discuss opportunity development more in a future strategic planning whitepaper, but a quick summary here illustrates the point.

Context. Just as with risk, we cannot identify a universe of opportunities, we must first define the context. What are we trying to do?

Opportunity Identification. Here we are brainstorming all opportunities within the context defined.

Opportunity Analysis. This step involves an understanding every element of the opportunity such as product or service need, industry maturity, market penetration, competition, etc.

Opportunity Evaluation. Then we look at how the opportunity will play out within the organization. For instance, does it fit within our core competencies, do we have the systems and resources to execute, what is the return on investment and profit margin, and can we differentiate from our competitors.

Monitoring & Review. Review in this context is tied to project management, sales, and numerous other KPIs relevant to the opportunity.

From an operational perspective, the intrinsic value of ERM is the synergy created when highly competent, effective and efficient management systems exist, the organization spends less time managing crises and more time managing the operation. Putting out little fires here and there (or daily – don't lie), with a bit of calamity thrown in every month or two may seem minor, but in realty it eats away at the time available for strategic thinking and planning. Forget for a moment the value of efficiencies gained, and the improvements captured when smart people get creative at solving problems, and the bottom-line expense reduction due to better process and fewer predicaments. When the organization is stable, it becomes proactive, nimble and able to seize upon opportunities because i) it is looking for them, ii) it has the resources to pursue them, and iii) it knows it can execute successfully. This is the gold ring for organizational success, and an ERM discipline together with integrated strategy and resiliency competencies will get you there.

When the organization is stable, it becomes proactive, nimble and able to seize upon opportunities.

Getting Started

Many of the tools and concepts discussed in this white paper are intentionally written for the executive level. While traditional risk management may function for your organization as an operational silo, achieving ERM competency requires an enterprise-wide approach that not only considers but actively integrates with strategic planning and business resiliency programs. This is a significant paradigm shift for most organizations and will not be successfully achieved from the middle. Thus, getting started means first and foremost a candid discussion at the executive (and possibly board level) of the problems the organization is experiencing and how they can be addressed with an ERM competency. This is where a project charter comes in handy, to capture the initial intent, purpose and objectives of the leadership team and to provide clarity to the staff assigned to do the heavy lifting.

Once a decision is made to pursue best practice capabilities, the next step is an internal scan. Chances are that your organization has some level of risk management, resilience and strategic planning practices in place. Take stock of how they function to map out a preliminary concept for how you envision the three will come together. This initial conceptualization work will help prevent re-work and redundancy later on. Next the discussion turns to more tactical matters of project plans, priorities, resources, budget, timelines and milestones. Remember, the most successful programs contain best practice elements, but the size, shape and color of your program will be very specific to your organization. Whenever possible, existing processes should be used – change for no reason is wasteful and undermines other legitimate improvements that can be made. Further, disruptive change is counter-productive and can easily result in delays (or worse, failure) than if the roll-out was thoughtful, measured and subtle.

Key Success Factor: Be Realistic – change takes time. The time it takes for an organization to reach ERM maturity (and thus resilience and strategy maturity) can range from one to five years, or even longer depending on entity size, program complexity and desired outcomes. Plan to build an internal multi-disciplinary team whose positions include, or will include, responsibility for program development and management. Utilizing consultants can help with things like program design, facilitation of risk appetite and tolerance discussions, and periodic audit and maturity assessments, but ultimately the competency should be internal to the organization. Recall Lesson One, Organizations = People. Your people are the first, best resource to accomplish ERM, and the key to ultimately realizing success according to whatever definition applies to your organization!

About the Author:

Erin Sedor is the talent behind Black Fox Strategy, a highly specialized executive consulting practice based on the philosophy that organizational success and sustainability are best achieved through integrated strategy, risk and resilience capabilities. Having built a 25-year career in the for-profit sector supporting, directing and successfully implementing strategic planning, enterprise risk, and business continuity programs, Erin now translates that experience into meaningful programs for her private, public and non-profit clients. Her broad industry background and deep expertise in balancing risk and opportunity makes her a uniquely qualified and valued asset to her clients.

Erin holds a Master's degree in Operational Risk, Bachelor degrees in Managerial Finance and Organizational Development, and is a RIMS Fellow Professional. She is an active member of the Risk & Insurance Management Society, Strategic Planning Association, Open Compliance & Ethics Group, and is a Certified Business Resilience Manager & Auditor.

Erin was born and raised in Alaska, and resides in Wasilla with Shawn, her husband of 25 years, where they raised their three amazing kids Nicole, Kyle and Jesse. Now, when they aren't working, they hang out with their dogs, Gibbs and JoJo, enjoying the beauty of Alaska.