Organizational Resilience

Managing the Risks of Disruptive Events – A Practitioner's Guide

James J. Leflar
Marc H. Siegel

CRC Press
Taylor & Francis Group

Organizational Resilience

Managing the Risks of Disruptive Events – A Practitioner's Guide

Organizational Resilience

Managing the Risks of Disruptive Events – A Practitioner's Guide

James J. Leflar
Marc H. Siegel


CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20130521

International Standard Book Number-13: 978-1-4398-4138-9 (eBook - PDF)

To my parents, Ann and James Leflar; my brother, Sam Leflar; and my niece, Rachel Pollock—gone, but never forgotten. And, to my sister, Ann, and my great nephew, Jack Pollock.

Jim Leflar

To my wife, Linda Zangwill, and my daughters, Dahlia, Maya, and Emma Siegel. And to my parents, Bernard and Irene Siegel.

Marc Siegel

CONTENTS

ACKNOWLEDGMENTS

When I started this project, several colleagues told me that it would be a labor of love; they were correct. I have always taken the approach that education is never ending and that opportunities to better myself are a fundamental aspect of being a professional. The material and value of this book are the product of years of experience, education, and interaction with my peers—I owe everything to their patience, guidance, and friendship. The very essence of this book is that one person is not capable of producing the level of synergy necessary to address the risk issues facing organizations. To my colleagues and friends who have helped me along the way, thank you.

Many years ago, I worked with the following Business Continuity Professionals and I gained a more robust understanding of BCP/DR through my interaction with them. To Mark Kern, John Sweeney, John Nones, and Steve Guss, thank you for bringing your business continuity "A" game each day. Through many "lessons learned," I saw what worked, and more importantly, what didn't work in a complex and changing environment.

Thank you to Jim Gallagher and Joan Burrell for being friends.

I would like to thank my friends for tolerating my excuses for neglecting them during the time I have spent on this project. Tony, I was responsible for the genesis of the Rhino joke. They say public confession is good for the soul, but I'm not convinced of that; I think that I just owe you the truth as your trusted ally. However, Rick played his part as the enabler and, in truth, no one objected; as I remember things, there was quite a bit of laughter. I hope that makes you feel better, Tony.

Several people deserve special attention because they have patiently assisted me in the actual development of this work. When I started on the path of developing this project, I sought suggestions from several colleagues and experienced authors on the best way to present the proposal. Richard Wright, James Lukaszewski, and Scott Watson helped get me started and I sincerely thank them for their guidance and friendship.

I was fortunate enough to work with Dr. Marc Siegel on the development of the ANSI/ASIS SPC.1-2009 Standard and I have called upon him many times during this project for assistance, eventually hooking him into helping write the manuscript. He has always come through and

given generously of his knowledge, time, and resources. I really owe an enormous debt to Marc and appreciate his invaluable assistance. His suggestions on improvements to this manuscript were insightful and helped elevate the final product in both clarity and accuracy. I do not think it is an exaggeration to say that this project would not have happened without his assistance.

Fortune smiled again and provided me with an opportunity to interact with Grant Lecky and Johan Du Plooy, with the result of some valuable information and feedback on this work. Johan provided his insights on actually implementing the ANSI/ASIS SPC.1-2009 standard in South Africa, along with his comments of the work herein. His contribution cannot be overstated.

Finally, a huge thanks to Mark Listewnik, Amber Donley, and Jay Margolis, my editors, for tolerating all my questions, concerns, suggestions, and their willingness to take a chance on me; it has certainly been an exciting trip.

I look forward to further adventures with all of these highly knowledgeable, thoughtful, kind, and professional friends.

Jim Leflar

I would like to thank Jim for giving me the opportunity to contribute to this work. I appreciate his patience in dealing with my frenetic travel schedule, especially not trying to phone me, which for me is almost always at some strange hour.

I would like to acknowledge the contributions that Susan Melnicove, Sue Carioti, and Aivelis Opicka have made to our profession. Without them there would be no ANSI/ASIS standards. They are truly the engine that drives the ASIS International standards program.

Special thanks go to Maya Siegel for her critiquing and editing the manuscript and not making too many jokes about me being English-challenged.

I would also like to thank my family, Linda Zangwill, Dahlia, Maya, and Emma Siegel, for their patience and understanding during the course of writing this book. I'm sure it had nothing to do with me telling them that they would be in the movie.

I hope this book inspires risk, security, crisis, and continuity managers to realize that in reality they are actually business managers helping to manage risk, security, crises, and continuity.

Marc Siegel

INTRODUCTION

SUPPORTING THE BUSINESS MISSION

Making assumptions is always a dangerous undertaking, but we shall take the gamble and assume that you are reading this book because you are either in a position to implement the information contained herein, or you are preparing for the possibility. In either case, this book shall provide valuable information that will allow you to succeed in moving an organization toward becoming more resilient through the use of organizational resilience management. Yes, the movement toward resiliency is a process and not a simple implementation of a policy or procedure. The analogy of a trip corresponding to implementing organizational resilience is appropriate and valuable. During a trip, you experience new ways of living, and learn to appreciate these new perspectives. You learn the value of doing things differently, and at looking at the world through a slightly different set of parameters. This is what happens when you begin to travel down the roadway of organizational resilience management; it is not a straight line, but a winding path requiring patience and tolerance. There is a good deal of learning that will have to take place during the trip and that is why it is necessary to have patience and tolerate the learning process. Old beliefs and habits will have to be modified into something new. That is part of the fun and adventure of taking this trip.

Organizational resilience is a goal to achieve and organizational resilience management is the way to achieve that goal. One of the real values of organizational resilience management (ORM) is that in developing and implementing this approach, there are further benefits in addition to the obvious intended result of implementation. Personnel learn to work together, they learn to appreciate and understand the concerns of other managers, and they gain experience by moving through the process of putting all the pieces together for a more resilient organization. Also, there is a shared experience derived from the participants going through the process of working on ORM that has real benefits in mitigating issues from becoming more serious. People learn to address issues in a more urgent fashion while minimizing negative consequences.

It is our sincere intent to provide a valuable and much-needed presentation that enables practitioners to achieve the desired goals of effective

organizational resilience through cost-effective methods. Building a resilient organization is a cross-disciplinary and cross-functional endeavor; therefore, "practitioners" may come from a variety of disciplines, all of which contribute to helping the organization achieve its objectives.

The primary goal of this book is to provide readers with an understanding of organizational resilience and how to manage risk through the use of the ANSI/ASIS SPC.1-2009 Standard. We shall endeavor to provide a concise, clearly understandable approach to successfully addressing the various challenges and techniques necessary to plan, prepare, and implement organizational resilience management in your organization. The reader will gain valuable insight into cutting through the complexities and identifying the key issues and techniques for successful implementation of organizational resilience management. The ANSI/ASIS SPC.1-2009 Standard is applicable to public, private, and not-for-profit organizations. This book focuses on organizational resilience management being an integral component of the overall business management of an organization. Organizational resilience needs to be seen within the context of protecting and creating value for the organization. Although the public sector has a mission and culture different from the private sector, many of the concepts and suggestions contained within this book can be used within the public arena. However, it is necessary to understand that benefits to the organization do not always translate equally from private to public.

INTRODUCTION TO THE ANSI/ASIS.SPC.1

A critical resource and the foundation for this book is the American National Standards Institute, Inc. (ANSI) approved ASIS International Standard on *Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use* (ANSI/ASIS SPC.1-2009). The standard is International Organization for Standardization (ISO) compatible with all management system standards to allow for seamless integration with ISO standards and to promote international relevance. The ANSI/ASIS SPC.1-2009 has been adopted by other countries (e.g., the Netherlands and Denmark) and served as the basis for the ISO 28002:2010 standard for resilience in organizations and their supply chains. In June of 2010, the U.S. Department of Homeland Security Public Sector–Preparedness Program (PS-Prep Program) approved ANSI/ASIS SPC.1-2009 for adoption as a national preparedness standard for private sector organizations, but adherence to the

PS-Prep Program is not necessary for use of the ANSI/ASIS SPC.1-2009 Standard and is not discussed in any detail in this book. The PS-Prep Program may be of value to some organizations and should be reviewed in more detail if a certification program is desirable for your organization. The PS-Prep Program is still in its infancy and the business value of the certification process has yet to be demonstrated. Remember, the goal of using any standard should be to enhance performance. The objective is to continually improve an organization's resilience and not to simply have a certification plaque hang on the wall of the main lobby of the corporate headquarters. Certifications are valuable if the reason and meaning for those certifications benefit the organization; we're looking for substance and not flash.

As the only ANSI-approved standard on organizational resilience management, it was a logical decision to use *Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use* (ANSI/ASIS SPC.1-2009) as the foundation for this book. It is reasonable to claim that this standard has been in development for many years in accordance with the development and evolution of planning for potentially disruptive events. Many disciplines address aspects of anticipating, assessing, preventing, protecting, mitigating, responding, recovering, and adapting to potential, undesirable, and disruptive events. Organizational resilience management is the result of many years of experiential knowledge and testing, culminating in a holistic systems approach that effectively blends the various risk issues necessary for achieving organizational resilience.

WHAT ARE STANDARDS?

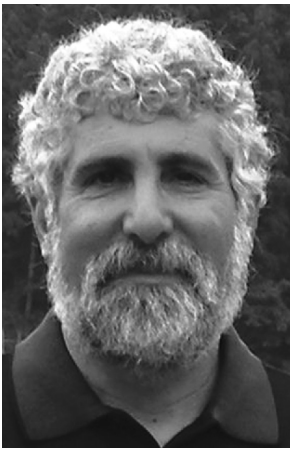
Standards impact our daily lives even if we don't notice them. We take for granted that our ATM card will work in bank machines around the world, that electronic components will be compatible in different devices, and chemical warning symbols can be understood regardless of your language. It is common to hear the term "standards" used in official and common language discussions, but there may be some confusion over the real meaning of the word. Standards are consensus-based specifications that define materials, methods, processes, services, or practices. A standard is not a regulation, rule, or law, but rather an agreed upon model that is used as a measure against which an outcome may be evaluated.

Standards help assure a defined, measurable, and consistent level of performance. They serve as tools to demonstrate a consistent and

acceptable level of quality, performance, and reliability. Management system standards, such as the ANSI/ASIS SPC.1-2009, specify a management process for what the organization does to manage its processes, services, or activities. It is like an Italian recipe; it tells you "what" you need to do, but lets you determine the "how" to fit your taste. A management system standard is not a checklist; it is a management framework viewed from the perspective that all the parts make up the whole. So, understanding the relationships and interactions between the elements of a management system is key to successful implementation.

ABOUT THE AUTHORS

James J. Leflar, Jr. (MA, CPP, CBCP, MBCI) is the security administrator at Johns Hopkins Bloomberg School of Public Health with responsibility for crisis management, business continuity, and security administration. He was an active member of the technical committees and working groups of the ANSI/ASIS SPC. 1-2009 and ANSI/ASIS SPC. 4-2012 standards. He continues to be active in OR standards development and is an active member of the ISO, U.S. Technical Advisory Group (TAG) 223 for Societal Security, Working Group 4—Preparedness and Continuity. Currently, Leflar is an active member of the ASIS International Crisis Management and Business Continuity Council as well as a member of the Advisory Board and Editorial Board for the Disaster Resource Guide.



Marc Siegel, PhD, is the commissioner heading the ASIS International Global Standards Initiative developing international and national risk management, resilience, security, and supply chain standards as well as providing training on their implementation. He is a RABQSA (Registrar Accreditation Board [RAB] Quality Society of Australasia [QSA]) international certified business improvement lead auditor as well as a certified trainer and skills assessor. As an adjunct professor in the College of Business Administration and the Master's Program in Homeland Security at San Diego State University, Dr. Siegel pioneered the concept of applying a systems approach to security and resilience management for organizations and their supply chains. His work includes providing training and guidance on the implementation

of risk, resilience, and security management systems as well as risk management in regions of conflict and weakened governance for the protection of assets and human rights. Dr. Siegel chaired the technical committee and working group for the ANSI/ASIS SPC.1: 2009.

1

Managing Risk to Optimize Performance

ORGANIZATIONAL RESILIENCE AND BUSINESS MANAGEMENT

Building a resilient organization is part of any good business management strategy. In order to thrive and survive, organizations need to adapt to an ever-changing environment. To be agile and resilient in order to achieve the organization's objectives, the organization needs to leverage all the disciplines that contribute to managing risk. For organizations to cost-effectively manage risk, they must develop balanced strategies to adaptively, proactively, and reactively address maximizing opportunities and minimizing the likelihood and consequences of potential, undesirable, and disruptive events.

Organizational resilience is a business management strategy that abandons the old approach of managing risk in siloed disciplines, but instead uses a multidisciplinary systems' approach to increase the adaptive capacity of the organization. The ANSI/ASIS SPC.1-2009 was the first standards initiative to buck the trend of what seems to be an endless stream of discipline specific standards being generated by ISO (International Organization of Standards). The ANSI/ASIS SPC.1-2009 views managing the risks of potential, undesirable, and disruptive events within the context of a single business management strategy as envisioned in the ISO 31000 risk management standard.

WHY MANAGE RISK?: THE BUSINESS CASE

An organization is primarily concerned with accomplishing operational goals that are aligned with and intended to achieve the strategic business goals. Examples of these goals are making a profit for a corporation or providing a service for nonprofit organizations. Typically, organizations have departments that are designed to protect the interests of the organization, e.g., security aims to protect against likely threats, and business continuity addresses the outcomes due to unacceptable business interruptions. The problem with these separate or silo approaches is that the separate department goals may be redundant and are not an efficient use of the limited resources available to achieve business goals. Department goals and practices must be aligned with the operational and strategic goals of the organization; otherwise, there is no legitimate reason for the goal. Having multiple departments working to achieve the same or similar risk-oriented goals is wasteful and counterproductive to those strategic goals. The convergence of these similar but disparate operations is best viewed as coming together through the thread of risk and resilience management. Risk management provides the underpinnings to allow security, crisis management, business continuity management, etc. to achieve consistent and thoroughly aligned strategies. The ability to assess and treat risk within the context of the organization's goals is the most efficient way to effectively consider risk.

Exhibit 1.1 is a partial list of typical risk sources and risk consequences. The risk source is something that has the possibility of creating uncertainty in the organization, preventing the organization from achieving its objectives, and may result in consequences to the organization. For instance, a thunderstorm may have consequences or it may simply go by without incident. The storm is the source of the risk and the loss of power is the consequence.

While it is important to adhere to the below mentioned principles, it also is important to have the obvious support and commitment from senior management to facilitate the development of the culture of risk management. (Note: the phrase "the management" is normally used in ISO standards language to reference the uppermost level of organizational management; top management and senior management are used interchangeably within this book.) This commitment is achieved through management policies, the assignment of resources to ensure continued operation of the risk effort, and the alignment of risk objectives with business objectives. It is absolutely essential to develop a culture that has risk management as one of the primary tenets.

List of Risks: Partial, not Comprehensive		
Category	**Risk Source**	**Risk Consequence**
Natural	Earthquake	Loss of Electricity Building Structural Damage Roadways Blocked – Damaged Fire
	Hurricane	Loss of Electricity Roadways Blocked: Flooding Water Damage to Building
	Lightning Strike	Loss of Electricity Computers Won't Operate Building Services Unavailable
	Snow Storm	Roadways Blocked Employees Can't Get to Work No Deliveries of Products or Supplies
	Thunderstorm	Loss of Electricity Roadways Blocked: Flooding Water Damage to Building
Man-Made	Electrical Equipment Failure	Loss of Electricity Building Technology Unavailable No Deliveries of Products or Supplies
	Labor Strike	Workers Strike – Work Flow Interruption No Deliveries of Products or Supplies Bad Publicity for Company
	Computer Virus	Computers Won't Operate Properly Services Unavailable to Customers Bad Publicity for Company
	Crime: Assault	Injury Increased Fear of Another Incident Negative Publicity – Reputation
	Hazardous Materials Incident	Fire Chemical Exposure Biological Exposure Radiological Exposure
	Accident – Personnel	Personnel Injured – Slip/Fall Lawsuit Negative Publicity – Reputation
	Accident – Vehicle	Property Damage Death – Injury Inability to Conduct Business

Exhibit 1.1 Risk sources and consequences table.

ISO 31000

All organizations face a certain amount of uncertainty and risk. In order to assure sustainability of operations and maintain resilience, competitiveness, and performance, organizations must have a system to manage their risks. The challenge is to determine how much risk and uncertainty is acceptable, and how to cost-effectively manage risk while meeting the organization's strategic and operational objectives. Given the finite resources of organizations, it is imperative to have business-friendly tools to address any array of threats, hazards, and uncertainties they may face. The ISO 31000:2009(E)—*Risk Management: Principles and Guidelines* standard is such a tool.

Risk management requires a thorough plan based on a comprehensive foundation to establish an enterprise-wide approach to understanding the organizational risks. The ISO 31000 provides guidance on the principles, framework, and process of risk management. It provides a generic perspective to managing risk that establishes a structure for organizations to integrate all of their risk management programs into a single framework. The document accurately reflects the current thinking that different disciplines of risk management should be considered in a comprehensive approach rather than "siloing" risks into separate approaches. This is the business sensible view of risk management, particularly important in these times of economic hardship and limited resources.

For organizations to cost-effectively manage risk, they should use the ISO 31000 in conjunction with the ANSI/ASIS.SPC.1 to develop balanced strategies to adaptively, proactively, and reactively address minimization of both the likelihood and consequences of potential, undesirable, and disruptive events, while also exploiting opportunities for improvement. The two standards will help an organization build a strategy for managing risk that is tailored to its business objectives that is also in sync with its overall goals and mission. It will provide the capacity for the organization to adapt to a complex and changing environment.

PRINCIPLES OF RISK MANAGEMENT

Any discussion of the ISO 31000 needs to begin with the definition of risk in the standard. Risk is "effect of uncertainty on objectives." According to the standard, "… an effect is a deviation from the expected"; therefore, risk can have either positive or negative outcomes. What seems like a

simple definition is actually a profound statement on risk management. Risk management is about achieving an organization's objectives. It is not event focused, but rather objectives focused. This means that risk managers are practicing their trade in a dynamic environment. There is a need for constant communication and consultation with stakeholders (the makers and owners of risk), constant monitoring of the environment, and situational awareness. In the ISO 31000 world, risk management becomes an integration of the preemptive strategies and discipline. With built-in feedback loops in every step of the risk management process, organizations learn and evolve based on input from their environment and context of operation. Obviously, because the risk management is practiced by humans (our apologies to other species), risk management is about adapting the organization as well as adapting the environment in which the organization operates.

Conformance with ISO 31000 depends on the adherence to the fundamental principles that risk management (ISO 31000:2009(E), pp. 7–8.):

- Not only creates, but also protects organizational value
- Is an integral component to all processes
- Is intricately intertwined with decision making
- Inherently focuses on the types and nature of the uncertainty facing the organization
- Is systematically designed to ensure reliable and consistent results
- Is structured and timely so that any information obtained is current and should lead to increased efficiencies within the organization
- Is conducted through the use of the best available multisourced information
- Is based on specific organizational needs; is part of the cultural fabric of the organization
- Involves all stakeholders and decision makers
- Is highly flexible, iterative, and change based
- Results in the organization benefiting from continual improvement

While it is important to adhere to the aforementioned principles, it is important as well to have the obvious support and commitment from top management and decision makers to facilitate the development of the culture of risk management. This commitment is achieved through management policies, the assignment of resources to ensure continued operation of the risk effort, and the alignment of risk objectives with business objectives. It is absolutely essential to develop a culture that has risk management as one of its primary tenets.

The principles of risk management establish the logic and justification for an organization to implement risk management. ISO 31000 establishes the desirability of following these principles when developing and implementing risk management within an organization. The principles are not necessarily specific to the risk management world; they, in fact, are sound business management principles applicable to all organizations and to any discussion on the implementation of an initiative. Any organizational initiative requiring the expenditure of resources must create value for the organization; otherwise, there is no justification for the initiative. A consistent theme throughout this book will be the alignment of any strategy, program, or standard with the organization. Everything that is done on behalf of the organization must be of value to the organization and achieve or lend in the achievement of the business goals. These principles are also inherent underpinnings of organizational resilience management, which is completely logical given the reliance SPC.1-2009 has on sound business and risk management principles.

ESTABLISHING A FRAMEWORK

In order to establish the risk management framework for an organization, it is necessary to understand the organization from both an internal and external perspective. This requires an appreciation of both the internal and external context in which the organization exists (ISO 31000:2009(E), p. 10). All organizations have an internal and external environment; the internal environment contains the activities, culture, and personnel (everything and everyone) within the organization. The external environment contains but is not limited to supply chain partners, supply vendors, clients, consumers, constituents, contractors, service technicians, transportation systems, regulators, the legal system, and governments. Before any attempt is made to develop the framework, it is necessary to understand the organization. Identifying all relevant stakeholders is essential for a successful consultative process. Developing the framework will become much easier and more valuable to the later risk management development activities.

Key to any risk management process is establishing the risk criteria. The risk criteria provide the terms of reference upon which risk will be evaluated and prioritized. Risk criteria are a function of the internal and external context, legal and regulatory obligations, and organizational objectives. Sounds easy? It's not. Trying to ascertain an organization's

level of risk acceptance and tolerance will be one of the most difficult tasks you will face in developing a risk management strategy. Risk criteria need to be defined with the intimate input of senior management in order to reflect the organization's value chain, objectives, resources, mission, and culture. Because risk management is supporting the achievement of the organization's objectives, and a tool to protect and create value, you must have a clear idea how you are going to calibrate the tool before using it; defining risk criteria provides the necessary calibration. Like any sensitive tool, recalibration is sometimes necessary. You should revisit the assumptions you make in defining the risk criteria when you are conducting the risk assessment.

The framework for the risk management process proposed in the ISO 31000 looks very similar to the Plan-Do-Check-Act model from the Total Quality Management approach to business management. The proposed framework is not specific to any one type of organizational design, but rather general in nature and allows the organization to create the necessary framework to properly function within the respective organization. The first step to establish the organizational mandate and commitment to support risk management within the organization. Obviously, without buy-in from management and decision makers within the organization, a risk management program cannot succeed. Buy-in is more than just a pat on the head; it involves a commitment to integrate risk management into all the organizational processes. This means senior management needs to be involved in creating a risk management policy and providing adequate resources. While this may appear to be a simple issue, it is not simple, and not all organizations will appreciate the need or value of risk management. Practitioners often hear senior leaders claim that they already have a risk management program (insurance) and anything more is unnecessary. While insurance is an option to treat a risk and is actually the transfer of risk from the organization to an insurance company, it is not a risk management program. Leadership must acknowledge and embrace risk management if it is going to succeed at a given organization. For risk management to be successful, it must become part of the organizational culture and this absolutely requires support and commitment from leadership in the form of a risk management policy. Without mandate and commitment, the risk management policy will not succeed.

Once a mandate and commitment is obtained, the organization can begin designing the framework for managing risk. This step sets the tone, context, and infrastructure needed to support risk management.

As discussed above, understanding the organization and its internal and external context provides the foundation on which you will build the house. The policy will establish the importance of risk management within the organization and, therefore, must be in alignment with the business goals, risk objectives, planned implementation strategy, and the organizational culture (ISO 31000:2009(E), p. 9). This alignment shall engender the active involvement of employees—risk management shall become part of their jobs: the risk makers and takers are the risk owners. To gain the involvement of the employees, risk must become an inherent responsibility of each person. Therefore, risk management is woven into the fabric of each position while they are performing their jobs. Furthermore, the organization's culture should be one of risk management and each risk strategy must be aligned with the business goals of the organization (ISO 31000:2009(E), p. 9).

Designing an organizational framework for managing risk must be tailored to fit the organization. Appropriate resources, including human resources, support a framework. The organization needs to identify competent people who will be responsible and accountable for managing risk. Identifying appropriate roles and responsibilities will build upon the information gathered during the policy and contextual understanding development phase, which then provides the basis for the organizational structure for risk management. Stakeholders involved in risk management should receive the necessary responsibilities and authority through specified duties in their respective job descriptions to promote success. Identification and procurement of the necessary organizational, human, training, monetary, physical, and informational resources are needed to support the framework. Risk management needs resources to fuel the process. Risk management also needs to become part of all the organization's practices and processes to run smoothly. Good communications, consultation, and monitoring are essential to supporting a dynamic framework. Good risk management practice is based on good information flow. The organization needs to establish the necessary communications protocols and mechanism capable of providing timely information to internal and external stakeholders in both normal and abnormal operating conditions. Remember that risk management is supporting the business management of the organization; therefore, information flow, control, and integrity all need to be considered when developing communication and reporting mechanisms.

The reason for designing a framework is to provide the infrastructure needed to implement the changes. Having defined the context of the

organization, the organization is now ready to apply the policy and risk management processes throughout the enterprise. When defining the timing and strategy for implementing the framework to manage risk, it is important to remember that the key reason for doing risk management is to support the organization in its quest to achieve its objectives—to create and capture value. Therefore, when building the implementation approach and setting the goals of the risk management process, the practitioner needs to align the outcomes with the organization's objectives, needs, and resources.

Monitoring and performance evaluation will let the organization know if its planning and implementation strategy is working. Situational awareness and ongoing monitoring of changes in the context and environment enable the organization to determine if the risk management approach is relevant in the nonsteady state environment that is the reality for most organizations. Risk management performance is measured in terms of the risk management supporting organizational performance. Identifying deviations from the plan and changing internal and external context should be seen as a learning experience and should pave the way for the organization to adapt its plans for risk management, and even change its business management approach to meet new challenges.

Dynamic organizations adapt, grow, and mature. Continual improvement is the underlying assumption of the risk management framework. Adversity and deviations from the risk management plan should be seen as opportunities for improvement and a means for strengthening the organization. The review of the framework should look at the adequacy of the framework, the need for making both minor and major adjustments, and, most of all, opportunities for improvement.

THE RISK MANAGEMENT PROCESS

Through the use of the framework and knowledge of the organization, it is necessary to establish a process to truly understand the risks associated with an organization. Exhibit 1.2 illustrates the process described in the ISO 31000 as it applies to the ANSI/ASIS.SPC.1.

Because the risk management process is used with the ANSI/ASIS. SPC.1, it will be discussed in more detail in Chapter 6.

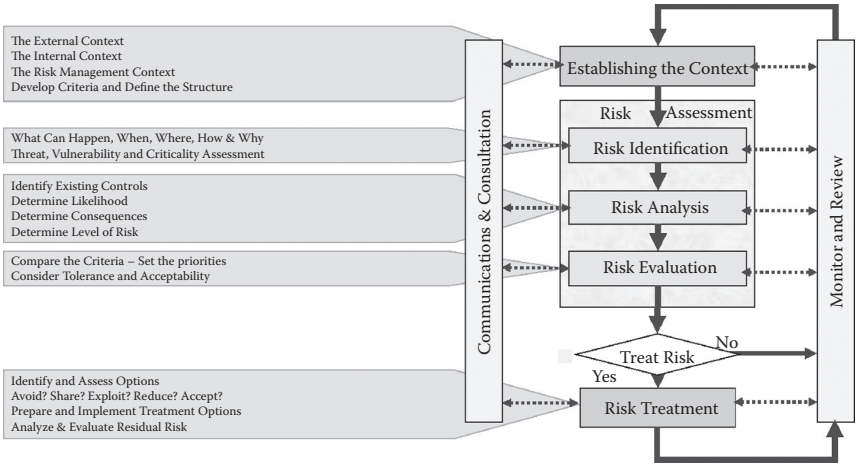


Exhibit 1.2 Risk management process diagram.

2

Managing the Risks of Disruptive Events

WHAT IS ORGANIZATIONAL RESILIENCE MANAGEMENT?

Organizational resilience (OR) is the goal that we are trying to achieve—making the organization more resilient and agile to risk-related issues. Organizational resilience management (ORM) is a risk-based management system applicable to all organizations: public, private, and governmental (ANSI/ASIS SPC.1-2009, p. vii). Organizational resilience management is how we are going to achieve organizational resilience.

Organizational resilience management is a cross-disciplinary, cross-functional approach to help an organization achieve its objectives. Change is inherent to any organization's operations; the environment in which an organization operates is in a constant state of flux. Therefore, to thrive and survive, organizations must be agile and adapt to internal and external changes in context. Ideally, organizations can anticipate changes and pre-emptively adapt. At other times, organizations need to learn from their experiences and adapt based on lessons learned. Some adaptations may be minor, while others may require significant adaptation of the organization's nature, character, purpose, or structure, even to the point of an organization reinventing itself.

Through the application of ORM principles identified in ANSI/ASIS SPC.1-2009, the managers of an organization have an excellent opportunity to develop a more resilient, risk management-oriented organization in

tune with the uncertainties and risks inherent to that organization. It is important to remember that ANSI/ASIS SPC.1-2009 does not attempt to deprive the organization of the qualities that make it special, but rather it provides the guidance necessary to reap the benefits of the ORM approach to achieving resilience.

The ISO Guide 73:2009—Risk management: Vocabulary defines resilience as "the adaptive capacity of an organization in a complex and changing environment." This is the same definition used in the ANSI/ASIS SPC.1-2009. In essence, resilience is the ability of an organization to change and adapt in order to handle challenges and/or issues. The better an organization manages to reorient itself to handle change and potential, and also undesirable and disruptive events, the more resilient the organization. Organizational resilience is not one activity or discipline; it is a state of being or condition as to the ability and capacity of the organization to anticipate, prepare, execute, and evolve. OR is not a reactive process, but rather a combination of various proactive activities through the careful implementation of organizational resilience management principles. It is absolutely crucial to understand that this resilience does not happen by mistake or chance. For an organization to become resilient, it takes planning and preparation; it takes a conscious effort to become resilient. Some readers may conclude that business continuity or crisis management are synonymous with OR. Both of these preparedness disciplines have goals that result in OR, but they are not the same thing. Business continuity focuses on planning and preparing for situations that would create unacceptable business process interruptions. "Crisis management identifies potential impacts that threaten an organization and provides a framework for building resilience, with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities as well as effectively restoring operational capabilities" (ANSI/ASIS SPC.1-2009, pp. 45–46). While both business continuity and crisis management strive to achieve a more resilient organization, they are not synonymous with ORM; they are pieces of the patchwork quilt that is ORM, a means to address risk and, therefore, aid in achieving resilience. Organizational resilience management is not a single discipline, but rather a blended consideration of the risks facing an organization. It is both a forward-looking and backward-looking approach to managing risk to achieve an organization's objectives. It is about maximizing opportunities and minimizing likelihood and consequences by removing the silos and finding the appropriate balance of adaptive, proactive, and reactive strategies.

Organizational resilience is a multidisciplinary systems approach to enhance an organization's adaptive capacity to enable it to manage and exploit risk to achieve its objectives. It is a collaborative process. The risk stakeholders within the organization (security, business continuity planning, asset management, human resources, business leaders, etc.) are the major stakeholders that must work together to develop the strategy and plans to achieve organizational resilience, but any strategy that is developed must be aligned with the business. Organizational resilience management is a management framework for action planning and decision making needed to anticipate, prevent (if possible), and prepare for and respond to changes in the environment and to events. It enhances an organization's capacity to prevent, manage, and survive undesirable events. It provides decision-making tools for organizations to take all appropriate actions to help ensure the organization's continued viability by anticipating, assessing, learning, and changing. Resilience is achieved through the contribution of a wide range of disciplines emphasizing the organization's capacity to adapt to potential adversity to minimize the likelihood of an event and use adversity for change and improvement. Organizational resilience management increases an organization's ability to achieve its objectives in the face of uncertainty and adversity as well as during nonroutine times. Organizational resilience complements quality, environmental, and occupational health and safety management, which ensures quality outcomes in routine and consistent operating environments.

The management systems approach of the ANSI/ASIS SPC.1-2009 encourages organizations to analyze organizational and stakeholder requirements and define processes that contribute to success. The ANSI/ASIS SPC.1-2009 Standard has conformance requirements that are designed to foster an understanding of the interrelatedness of the organizational business units, the viewing of functional requirements to achieve business unit viability and success, and the understanding of the myriad business unit perspectives of risk. The Standard attempts to generate increased understanding of the processes internal and external to the organization from a risk perspective. This also is always from an organizational business needs perspective. Through achieving this understanding and the implementation of the conformance requirements, an organization has greatly increased its chance of achieving OR.

Simply following the OR Standard does not guarantee success. The organization must accept the concept of breaking down the established barriers for protecting individual managerial kingdoms (functional silos)

Exhibit 2.1 Organizational resilience challenge diagram.

and actively seeking joint approaches to addressing risk through the realization that organizations are comprised of interrelated, interdependent operations. Exhibit 2.1 is an example of the organizational resilience challenges facing a university, but with slight modifications (changes in stakeholders to reflect those of a particular organization) could be an example of any organization. The diagram shows various stakeholders or attitudes coming into play, focusing on their respective issues, but without the benefit of a unified position or an understanding of other stakeholder positions. Some of the challenges are actually attitudes that must change before any serious improvement in OR can be realized. The old adage: "We've never had any trouble before," is a serious failing that is all too common. Most experienced risk management and preparedness professionals have probably heard this during their careers. While it is prudent and appropriate to carefully consider the risk and the likelihood of occurrence, it is not appropriate for managers to hide from the real possibility of an incident affecting the organization. Preparing for the unexpected, unacceptable, and ill-timed emergency is the duty of every manager. There are constant changes in the operating environment and threats facing an

organization and the resulting risks, which may never have happened at an organization before, should be considered as potential issues.

RELATIONSHIP BETWEEN THE ISO31000 AND ANSI/ASIS.SPC.1

The ISO31000 was a major breakthrough in the world of risk management. The Standard provides clearly described principles, a framework, and a process for risk management. It shifts the view of risk from bad things that go thump in the night (a focus on events) to uncertainties in achieving an organization's objectives. By moving from event-focused to objectives-focused, the organization moves from reactive mode to proactive mode. Risk management becomes about creating and capturing value rather than just protecting value. Risk management is about foresight and strategic planning.

The perspective that risk management is a consultative and collaborative process means all risk owners are risk managers. Risk management is an inclusive process, top-down and bottom-up. The ISO31000 also emphasizes that managing risk is cross-disciplinary and cross-functional throughout the entire enterprise.

The ANSI/ASIS.SPC.1 follows the thinking of the ISO31000. Organizational resilience is not about "bouncing back" or just protecting the organization; it emphasizes that organizational resilience is about protecting, creating, and capturing value before, during, and after an event. The ANSI/ASIS.SPC.1 takes the same cross-disciplinary and cross-functional approach as the ISO31000 and views the need to leverage all the risk-focused disciplines to build a single business management strategy for addressing risks related to potential, undesirable, and disruptive events.

The ANSI/ASIS.SPC.1 builds on the ISO31000 by highlighting the notion that being resilient depends on the organization's capacity to adapt. To maximize opportunities and minimize likelihood and consequences, organizations must be ready to be agile in changing conditions and adapt before, during, and after an event to either prevent the event from occurring or learning from the event to realign itself, or even reinvent itself, in order to fit its new environment. Organizational resilience is truly about an organization's capacity to adapt to a complex and changing environment.

RESILIENCE FROM A FUNCTIONAL AND OPERATIONAL PERSPECTIVE

Although organizations, small and large, share similar concerns surrounding the management of risks and the protection of the business, the difference is often in the level of complexity within the business organization to address that concern. Addressing risk is an expectation that clients, shareholders, business partners, regulators, and employees have of any organization, regardless of size. At first glance, it might seem that smaller businesses are at a disadvantage to implement an organizational resilience management system; however, the converse may be true. Smaller businesses may have one person handling multiple responsibilities, while major corporations have numerous departments dedicated to providing the necessary protective measures. Therefore, smaller businesses might not have divisional and discipline silos. It seems obvious that an organization must address risk, but recent financial industry revelations have shown that not all risk is identified or, worse, it is simply ignored. Eliminating the silos and assessing risk from a multidisciplinary perspective will help an organization better prioritize resources to protect itself from anticipated and unexpected events. By focusing on the achievement of objectives, organizations are better positioned to adapt to changes, if not by anticipating and adapting before the fact, at least learning from events to adapt and strengthen and grow the organization. Seen from this perspective, organizations can effectively manage uncertainty and capture or realize any opportunity.

One of the challenges involving risk is that many organizations are established on a functional basis. Each business unit is separate from the others and often reporting to different leaders without the benefit of any consistent, unified management structure focusing the resources toward risk management. For instance, safety, risk management, financial operations, security management, business continuity management, information technology disaster recovery, information and network security, corporate communications, corporate counsel, and crisis management are a few of the leading disciplines involved in protecting a business. It is common to think of the above disciplines as independent "professions" because they are marketed that way as courses of study in college and professional organizations with assorted certifications indicating specialized training and achievements. All of that is fine and valuable, but it creates the expectation that risks and threats against an organization fall into categories addressed by certain disciplines within the business. For

instance, certain criminal issues, such as theft of information and proprietary secrets, may fall into the physical and/or information security realms, while crisis management and/or business continuity management might consider the consequences of the theft. Considering the business needs to manage the integrity of its information, rather than each discipline separately, a more reasonable approach is to "blend" the preventative measures, preparations, and response so that more than one department is involved in the resolution. This avoids duplication of efforts and provides a comprehensive strategy to prevent the loss of an asset. An incident often affects multiple stakeholders; therefore, having those stakeholders work together before an incident occurs allows for a more dynamic and, hopefully, preemptive approach to the issue. Complex issues require more complex approaches to achieving a resolution. For instance, when a disgruntled employee is investigated concerning allegations of harassment, it is necessary to include multiple "risk" stakeholders to determine the full measure of risk. Viewing the issue as a simple human resources problem that is resolved by firing the person fails to acknowledge the risks due to retaliation to both personnel and property assets of the organization. It is necessary to include at least human resources, physical security, data security, the department manager of the employee, and any other appropriate stakeholders (e.g., mental health professionals) that your organization may have that will help develop a full picture of the risk. In addition, the team needs to understand a key precept of organizational resilience—an incident avoided or prevented does not become a crisis. While preemptive adaptation may avoid a problem from materializing, nevertheless, the organization should always assess how it can further adapt and evolve in order to avoid similar threats of adversity in the future.

It is quite true that many risk issues require the talents of specialists to effectively understand and address, but this separation of duties is also part of the problem. All too often, risk management operations are organized as completely discrete business operations with separate goals and perspectives. This "silo" approach to operations is detrimental to effective comprehensive risk management efforts. Organizational resilience management is a systematic, enterprise-wide approach that fosters the inclusion of different risk management-oriented disciplines as noted above, thus, creating a synergy not realized with disparate approaches. ORM does not seek to replace or eliminate any department or discipline within an organization, but rather seeks to include all disciplines to gain a more effective and efficient risk resolution operation. This inclusive risk-based approach allows for preparedness at the

earliest stages, thereby preventing an issue from becoming a more serious concern. For example, an organization's main data center should have a number of risk managers as stakeholders. All stakeholders work together to address the various concerns, such as data security and maintenance of servers (Information Technology), electrical and HVAC (Facilities Management), physical security (Corporate Security), space planning (Corporate Real Estate/Facilities), compliance (Risk Management), etc., and a variety of third-party vendors performing other duties. All of these stakeholders have a vested interest in developing an integrated approach to managing the risk of the data center instead of independent approaches.

The actual organizational structure also may lead to the aforementioned silo effect more often than any philosophical approach to addressing duties. If departmental managers report to different senior managers, the issue may be as simple as disparate perspectives: competing priorities (and budgets), lack of a perceived problem, or organizational politics. The functional divisions in Exhibit 2.2 are examples of possible "silo" causing situations, and Exhibit 2.3 is an example of how to avoid those silos. This example may not be feasible in some organizations because this level of change almost always only happens from the senior-most leadership. Gaining a senior-level sponsor is not only helpful; it is critical if this sort of change is being considered.

Exhibit 2.2 is an example of an organization with a more "silo" type of approaching risk issues. Each division consists of a number of departments

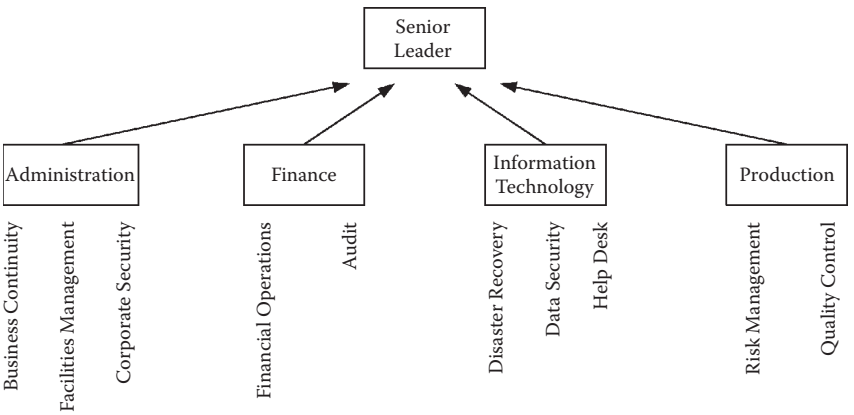


Exhibit 2.2 Silo structured example of organization.