October 2014

Fundamentals of Risk Management | Michael McCormick

Contents

KEY OBJECTIVES 5
Purpose (To Propose) 5
Audience 6
Introduction 6
Organizational Risks 6
Sound Decision Making 7
Risk Management Value 7
Risk Management Applications 8
Strategic Planning 8
Capabilities-based Planning 8
Resource Decisions 8
Operational Planning 8
Exercise Planning 9
Real-world Events 9
Research and Development 9
RISK MANAGEMENT PRINCIPLES 9
Principle Descriptions 10
Risk Maturity Levels 12
Risk Maturity Levels 12
Level 5: 12
Level 4: 12
Level 3: 12
Level 2: 13
Level 1: 13
The RISK MANAGEMENT APPROACH 14
Table 1: Organizational Risk Categories 15
Key Business Practices 15
Driving Risk Results 16
Enhance Risk Strategy 16
Embed Risk Management 16
Optimize Risk Management Functions 17
Improve Controls and Processes 17
Enable risk management, communicate risk coverage 18

Contents Continued

GRC Fundamental Component: Risk Ontology 19
What is Risk Ontology? 19
What's in a Risk Framework? 19
Risk Framework: Five Easy Steps 20
Enterprise RISK MANAGEMENT (ERM) 21
ERM Matrix Chart 22
The RM Process 22
Risk Communications 23
Elements of the Risk Management Process 24
1. Define the Context 24
1.1 Goals and Objectives 25
1.2 Mission Space and Values 25
1.3 Policies and Standards 25
1.4 Scope and Criticality of the Decision 25
1.5 Decision Makers and Stakeholders 26
1.6 Decision Timeframe 26
1.7 Risk Management Capabilities and Resources 26
1.8 Risk Appetite 26
1.9 Risk Tolerance Levels 27
1.10 Availability and Quality of Information 27
The ERM Design Approach 27
2. Identify Potential Risk 29
2.1 Unusual, Unlikely, and Emerging Risks 29
2.2 Scenarios 29
3. Risk Assessments 30
3.1 Methodology 30
3.2 Types of Methodologies 31
3.3 Collecting Data 31
3.4 Validation and Presentation 32
3.5 Integrating Alternatives 32
4. Develop Alternatives 33
4.1 Identifying Options 33

Contents Continued

4.2 Risk Management Strategies 33
4.3 Methods for Alternatives 34
4.4 Requirements and Constraints 34
4.5 Iterative Process 34
5. Decide Upon and Implement Risk Management Strategies 35
5.1 Presenting Information 35
5.2 Document and Implement 35
6. Evaluation and Monitoring 36
6.1 Performance Measurement 36
6.2 Logic Models 36
6.3 Models of Evaluation 37
7. Risk Communications 38
Enterprise Risk Modeling 41
VoR Modeling 42
Corporate Risk Modeling Tools 42
In Closing 43
The Author 43

KEY OBJECTIVES

The application of Risk Management (RM) fundamentals are intended to help organizational leaders, supporting staff, managers, analysts, and operational personnel with developing a framework to make risk management an integral part of planning, preparing, and executing organizational missions.

The development of organization's risk management framework is an essential element in promoting a risk-informed culture enabling training, capability development, and integration across the organization to strengthen and improve the organization's long term viability. Risk Management fundamentals articulates a desired end-state that organizations should aspire to achieve in promoting risk management.

The author's viewpoints are not a substitute for independent thought or innovation in applying these principles and concepts. Simply reading this whitepaper will not make one adept in managing risks, nor will attempting to follow the ideas herein as if they were a checklist; rather, the whitepaper serves to shape how one thinks about the issues that you are considering and should be applied based on the operating environment.

The Application of Risk Management whitepaper captures the theoretical underpinnings of organizational risk management and articulates principles and practices that should be strived for across organizational decision making. In doing so, this document should not be read as criteria to be evaluated against, but instead as a statement of aspirations for improved organizational decision making, applied in a variety of operating environments, many of which face constraints. Organizational practitioners should compare this whitepaper herein against their own experience and think about why, when, and how it applies to their situation and area of responsibility.

Purpose (To Propose)

The purpose of this document is to:

- Promote a common understanding of, and approach to, risk management;
- Establish organizational practices that should be followed;
- Provide a foundation for conducting risk assessments and evaluating risk management options;
- Set the fundamental underpinning for institutionalizing a risk management culture through consistent application and training on risk management principles and practices; and
- Educate and inform organizational stakeholders in risk management applications, including the assessment of capability, program, and operational performance, and the use of such assessments for resource and policy decisions.

Audience

The principal audiences for *Risk Management Fundamentals* are DHS employees, including*:*

- Executives who establish strategic and operational priorities, select courses of action, and allocate resources;
- Program Managers and Planners who turn executive decisions into actionable, implementable plans and oversee the day-to-day execution of these plans;
- Operational Personnel who implement plans and programs using specific, tactical and operational risk management tools; and
- Risk and Decision Analysts who collect, assess, and present risk information to help executives make decisions, aid program managers and planners in explaining decisions and approaches to stakeholders, and assist operational personnel in connecting their work to the desired outcome.

INTRODUCTION

Organizational Risks

The organization's environment that is complex and filled with competing requirements, interests, and incentives that must be balanced and managed effectively to ensure the achievement of key objectives. The safety, security, and resilience of the organization are threatened by an array of hazards, including acts of terrorism, malicious activity in cyberspace, pandemics, manmade accidents, transnational crime, corruption and natural disasters.

At the same time, organizations must manage risks associated with workforce management, ecommerce, acquisitions operations, and project costs to name a few. Collectively, these external and internal risks have the potential to cause loss of life, injuries, negative psychosocial impact, environmental degradation, loss of economic activity, reduction of ability to perform mission essential functions, and loss of confidence in organizational capabilities.

It is the role of the organization to understand and manage these myriad risks. We live in a dynamic and uncertain world where the past does not serve as a complete guide to the future. In addition, the systems that provide the functions essential for a thriving society are increasingly intricate and interconnected. This means that potential disruptions to a system are not fully understood and can have large and unanticipated cascading effects throughout organization.

Compounding this complexity is the fact that future trends — such as technological advancements, global climate change, asymmetric threats, and the evolving nature of the global economy — have the potential to significantly alter the organization's risk landscape in unexpected ways. Yet such emerging trends hold promise as well as peril and should be understood and managed.

Sound Decision Making

Establishing the capability and capacity to identify, understand, and address such complex challenges and opportunities is the crux of risk management. Risk management is an approach for making and implementing improved organizational decisions.

The application of Risk Management is the process for identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any decisions enacted.

To improve decision making, organizational leaders must practice foresight and work to understand known and uncertain risks, as best they can, in order to make sound management decisions. These leaders need to consider the risks facing the organization to make appropriate resource tradeoffs and align management approaches.

Risk Management Value

At the organizational level, the application of risk management will complement and augment strategic and operational planning efforts, policy development, budget formulation, performance evaluation and assessments, and reporting processes.

Risk management will not impede adverse events from occurring; however, it enables organizational efforts to focus on those things that are likely to bring the greatest risk impact, and employ approaches that are likely to mitigate or prevent those incidents. Furthermore, the organization is made more resilient by anticipating, communicating, and preparing for catastrophic events, both internal and external, through comprehensive and deliberate application of risk management.

Risk management is not an end in and of itself, but rather part of sound organizational practices that include:

- Planning,
- Preparedness,
- Program evaluation,
- Process improvement, and
- Budget priority development.

The value of a risk management approach or strategy to decision makers is not in the promotion of a particular course of action, but rather in the ability to distinguish between various choices within the larger context. One of the foundational concepts for organizations is the need to build resilient systems, committees, and practitioners that are robust, adaptable and have the capacity for rapid recovery. Resiliency and risk management are mutually reinforcing concepts.

Risk management contributes to the achievement of resilience by identifying opportunities to build resilience into planning and resourcing to achieve risk reduction in advance of a hazard, as well as enabling the mitigation of consequences of any catastrophic event.

Establishing the infrastructure and organizational culture to support the execution of an organization's risk management is a critical requirement for achieving the organization's RM goals. Risk management is essential for organizational leaders in prioritizing competing requirements and enabling comprehensive approaches (the science) to measure performance and detail progress.

Risk Management Applications

The practice of risk management allows for a systematic and comprehensive approach to organizational decision making. Risk management promotes the development and use of risk analysis to inform organizational decision making, to better inform selection among alternative strategies and actions, and to evaluate the effectiveness of the activities undertaken.

Risk management applications include:

Strategic Planning

Organizational strategies should be designed to address the risks that a particular organization faces, taking a long-term view to building capabilities that can mitigate risk through prevention, protection, response, and recovery activities. Organizational strategies should shape how organizations approach building and sustaining capabilities.

Capabilities-based Planning

Risk management allows planners to prioritize which capabilities might have the greatest return on investment in preparedness activities. Risk management can also help identify which capabilities are most relevant to an organization and identify potential capability gaps.

Resource Decisions

Risk management should be a key component of an evidence-driven approach to requesting and allocating resources. By understanding risk, organizations can identify realistic capability requirements, fund projects that bring the greatest return on investment, describe desired outcomes and how they will mitigate risk, and explain the rationale (the Art of Science) behind those decisions in clear, objective, and transparent terms.

Operational Planning

Through risk management, organizations can better understand which scenarios are more likely to impact them, what the consequences would be, what risks merit special attention, what actions must be planned for, and what resources are likely to be needed, as well as what risks have the ability to negatively impact operations.

Exercise Planning

Risk management can be used to identify realistic scenarios for exercises, zeroing in on special threats and hazards, as well as priority capabilities and applicable assets.

Real-world Events

Risk management can help decision makers weigh potential courses of action within a contextual understanding of the risk of different threats and hazards to critical assets, geographic areas, and population centers during a crisis.

Research and Development

Risk analysis can be used to inform decisions on filling organizational gaps and identifying opportunities that may be best met with enhanced technologies and/or innovative solutions, thereby establishing priorities for long-term research and development investments.

RISK MANAGEMENT PRINCIPLES

Risk management enables organizational leaders to distinguish between and among alternative actions, assess capabilities, and prioritize activities and associated resources by understanding risk and its impact on their decisions.

Standard risk management principles are not designed to promote uniformity or conformity; rather, they offer broad guidance that should be uniquely tailored for the specific needs of each organization. While a “one-size-fits-all” approach for the organization’s risk management is neither feasible nor desirable, all risk management programs should be based on two key principles:

1. Risk management should enhance an organization’s overall decision making process and maximize its ability to achieve its objectives.

2. Risk management is used to shape and control risk, but cannot eliminate all risk.

The key principles for effective risk management should include:

- Culture of Effort
- Transparency
- Adaptability
- Practicality
- Customization

Principle Descriptions

Culture of Effort: *The principal of culture of effort (risk appetite) reiterates that organizational risk*

Risk management efforts should be coordinated and integrated among all partners, with shared or overlapping risk management responsibilities, to include local or Federal governments, as well as the private sector, non-governmental organizations, and international partners. Most organizational measures involve representatives of different organizations (e.g. Insurance Companies), and it is important that there is unity of effort amongst those charged with managing risks to ensure consistent approaches are taken and that there is a shared perspective of risk challenges.

Transparency: *The principle of transparency establishes that effective organization's risk management depends on open and direct communications*.

Transparency is vitally important in organizational risk management due to the extent to which the decisions involved affect a broad range of stakeholders. Transparency is important for the analysis that contributes to the decision making. It includes the assumptions that supported that analysis, the uncertainty involved with it, and the communications that follow the decision. Risk management should not be a "black box" exercise where analysis is hidden. Those impacted by a risk management approach should be able to validate the integrity of the approach.

This principle does not revoke the times when there is need for security of sensitive or classified information; however, it does suggest that the processes and methodologies used for organizational risk management may be shared even if the information is not. In turn, transparency will foster honest and realistic dialogue about opportunities and limitations.

Adaptability*: The principle of adaptability includes designing risk management actions, strategies, and processes to remain dynamic and responsive to change through continuous maturity level assessments*.

The organization's landscape is constantly evolving as priorities, threats, and circumstances change, requiring the organization to adapt to meet the expectations and requirements. The organization must be flexible in their approach to managing risk. This means that organizational solutions must be dynamic. A changing world, filled with adaptive adversaries, increased interdependencies, and new technologies, necessitates risk and security measures that are equally adaptable.

Practicality: *The principle of practicality pertains to the acknowledgement that organizational risk management cannot eliminate all uncertainty nor is it reasonable to expect to identify all risks and their likelihood and consequences.*

The limitation of managing organizational risk arises from the dynamic nature of organizational threats, vulnerabilities, and consequences, as well as the uncertainty that is generally associated with assessing risks. This is especially true when facing a threat from an adaptive adversary, such as cyber security threats from employees, external individuals, organizations or foreign countries.

Organizational decisions often are made amidst uncertainty, but that uncertainty does not preclude the need for useful analysis or well thought-out and structured decision making. Risk management is an effective and important management practice that should lead to better-supported decisions and more effective programs and operations.

Customization (Maturity Level): *The principle of customization emphasizes that risk management programs should evolve (Risk Maturity Levels) to match the needs and culture of the organization, while being balanced within the specific decision environment they support*.

Organizations and personnel should tailor the methods for the dissemination of risk information and decision making and communications processes to fit the needs of their mission. The customization principle includes ensuring that the organization's risk management approach is appropriately governed and uses the best available information. This assures that the risk management effort is systematic, timely, and structured based on the values of the organization. However, the principle of customization does not supersede the need to adhere to organizational standards, requirements, and operating procedures for risk management when there is a requirement for working together to analyze risks and promote joint decision making.

RISK MATURITY LEVELS

Risk maturity levels consist of a predefined set of process areas. The maturity levels are measured by the achievement of the specific and generic goals that apply to each predefined set of process areas.

The 10 characteristics of risk maturity:

1. Organizational Understanding & Commitment to Risk Management
2. Executive Level Risk Management Stewardship
3. Risk Communication
4. Risk Culture: Engagement & Accountability
5. Risk Identification
6. Stakeholder Participation in Risk Management
7. Risk Information & Decision Making Processes
8. Integrating Risk Management & Human Capital Processes
9. Risk Analysis & Quantification to Understand Risk & Demonstrate Value
10. Risk Management Focus on Value Creation

Risk Maturity Levels

Level 5:

The organization that has developed the ability to identify, measure, manages and monitors risks; risk management processes are dynamic and adapt to changing risks and business cycles:

- Formal statements of risk appetite and tolerance exist and guide decision making
- Risk and risk management information is explicitly considered in decision processes
- Analysis is consistently applied, incorporating qualitative & quantitative techniques
- Risk management is viewed as providing a competitive advantage with a focus on optimizing risk-reward trade-offs

Level 4:

There is a clear understanding of the organization‘s key risks and also a consistent execution of activities to address these risks; some functional areas may employ more sophisticated techniques:

- The set of loss and tolerance guidelines are predetermined or developing
- Explicit consideration of risk and risk management information is taken in key decisions
- Analysis is consistently applied, incorporating both qualitative and quantitative techniques

Level 3:

The organization understands and is addressing its key risks; capabilities to measure, manage and monitor risks are in place but may be inconsistent across the organization:

- Guidelines for loss and risk tolerance are less developed
- Risk and risk management information is considered informally I implicitly in decision making
- Analysis is consistently applied, with a focus on qualitative approaches

Level 2:

There is inconsistent understanding, management and monitoring of key risks across the organization; capabilities to consistently identify, assess, manage and monitor risks are limited:

- Risk management activities occur at the functional level rather than the enterprise level
- Risk management activities emphasize compliance
- Risk and risk management information is considered informally or implicitly in decision making, often on an ad hoc basis

Level 1:

If the organization identifies and addresses risks it is done within silos only; components and activities of the risk management process are limited in scope and implemented in an ad-hoc manner.

THE RISK MANAGEMENT APPROACH

Organizational decision makers should employ a comprehensive approach to understanding and managing risks so that they can enhance the quality of decisions throughout their organization — thus supporting the a organizational policy for Integrated Risk Management. Doing so serves to improve decision making by allowing organizations to attempt to balance internal and external sources of risk to achieve their strategy. This section identifies the types of risks facing organizations, and sets forth some necessary practices for managing these risks in an understandable way.

Internal Sources of Risk

Risks impacting organizational effectiveness arise from both internal and external sources. Examples of internal sources are issues such as financial reporting, personnel reliability, and systems reliability. These internal risks have the potential to derail effective operations and adversely affect mission accomplishment. A comprehensive approach to risk management serves to identify weaknesses and assists in creating internal systems and processes that minimize the potential for mission failure.

External Sources of Risk

Many organizations have additional risks to manage that are caused by external factors. Examples include global, political, and societal trends, as well as hazards from natural disasters, terrorism, and malicious activity in cyberspace, pandemics, transnational crime, and manmade accidents. It is these hazards and threats that caused the Nation to make a significant commitment in homeland security, and it is important that the risks from external threats remain at the forefront of consideration for organizational organizations.

*"**Threat** is a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property."*

Organizations should implement comprehensive risk management approaches to ensure all internal and external risks are considered in a holistic way. Organizations must manage risks as a system, while considering the underlying factors that directly impact organizational effectiveness and mission success.

In order to consider the whole of organizational risks, the categories in the following ***Table 1*** (page 12) help to define the framework for an organization as it establishes a comprehensive approach to risk management. Identifying and understanding risks and their interactions ensures organizational leaders have a more complete perspective to manage risks and promote organizational effectiveness.

Table 1: Organizational Risk Categories

Risk Categories	Strategic Risks	Operational Risks	Organizational Risks
Definition	Risk that affects an organization's vital interests or execution of a chosen strategy, whether imposed by external threats or arising from flawed or poorly implemented strategy	Risk that has the potential to impede the successful execution of operations with existing resources, capabilities, and strategies.	Risk associated with an organization's ability to develop and maintain effective management practices, control systems, and flexibility and adaptability to meet organizational requirements.
Description	These risks threaten an organization's ability to achieve its strategy, as well as position itself to recognize, anticipate, and respond to future trends, conditions, and challenges. Strategic risks include those factors that may impact the organization's overall objectives and long-term goals.	Operational risks include those that impact personnel, time, materials, equipment, tactics, techniques, information, technology, and procedures that enable an organization to achieve its mission objectives.	These risks are less obvious and typically come from within an organization. Institutional risks include factors that can threaten an organization's ability to organize, recruit, train, support, and integrate the organization to meet all specified operational and administrative requirements.

Key Business Practices

Effective management of risk is fostered and executed through a few key requirements. First and foremost, an organization must employ risk management with commitment and active participation by its leadership. If decision makers within an organization fully endorse and prioritize risk management practices, then employees at all levels will strive to understand and adopt risk management principles. Furthermore, risk management is only effective if it is used to inform decision making. This means that for risk management efforts to be successful, leaders must support risk management practices and incorporate risk information into their decision making processes (e.g. Governance or Executive Committees).

Second, managing risk requires a consistent approach across the organization. Although processes do not need to be identical, they should facilitate the ability to compare risks, as required, across the organization and provide reasonable assurance that risk management can be conducted coherently. Managing risk as a system allows for greater situational awareness of how varied risks and mitigation efforts may impact other activities.

Third, an organization must be able to view risk on a comprehensive, enterprise-wide basis. Most risk information is viewed by the individuals responsible for managing particular risks, who are not necessarily able to see how risks can affect other parts of the organization or to see the cumulative risks the organization faces. Thus, an organization requires some sort of function that allows for information to cascade up, providing its leadership with an organization-wide view of its risks so as to promote better tradeoff decisions and enhance application of foresight.

Driving Risk Results

Organizations achieve results from risk in three interrelated ways:

- **Risk Mitigation:** In a worst-case scenario, an organization's risks can proliferate at a far faster rate than its ability to provide coverage. Organizations need to have the ability to identify and address key risk areas and the ability to quickly close the gaps.
- **Cost Reduction:** For many organizations, finding cost efficiencies in every facet of the organization continues to be critical to survival in this volatile economic environment.
- **Value Creation:** Many organizations are looking for ways where risk and control management can help improve business performance.

Enhance Risk Strategy

Effective risk management starts with clarity around risk strategy and governance. It is critical for companies to have proper oversight and accountability at the board and executive levels. An enhanced governance structure, board-level reporting and communications result in improved visibility, accountability, transparency and strategic decision-making.

Enhancing risk strategy enables organizations to more effectively anticipate risk. However, it is equally important to develop reactive strategies that enable the organization to respond quickly if a risk does materialize. Risk is inherent in every business.

- Two-way open communications about risk with external stakeholders.
- Transparent and timely communication, providing relevant information that conveys the decisions and values of the organization.
- The board or management committee plays a leading role in defining risk management objectives.
- A common risk framework has been adopted and implemented across the organization.

Embed Risk Management

Organizations that embed risk management practices into business planning and performance management are more likely to achieve strategic and operational objectives.

So what are top performers doing right?

- There is a formal method for defining acceptable risk thresholds within the organization.
- Stress tests are used to validate risk tolerances.
- Leadership has put in place an effective risk management program.
- Planning and risk reporting cycles are coordinated so that current risk information is incorporated into business planning.

Optimize Risk Management Functions

As an organization changes and grows, its risk, control and compliance activities often become fragmented, siloed, independent and misaligned.

This has an impact on both the governance oversight and the business itself.
By taking the following steps, an organization can reduce its risk burden (overlap and redundancy), lower its total costs, expand coverage and drive efficiency.

So what are top performers doing right?

- Completion of risk-related training is incorporated into individual performance.
- Risk monitoring and reporting tools are standardized across the organization.
- Integrated technology enables the organization to manage risk and eliminates or prevents redundancy and lack of coverage.
- Overlap and duplication of risk activities have been identified and are being addressed.

Improve Controls and Processes

Although organizations understand the value of building controls and processes that focus on risk, many organizations still struggle to create optimal control environments that balance cost with risk. By optimizing controls around key business processes, harnessing automated versus manual controls, and continuously monitoring critical controls and KPIs, organizations can improve performance and reduce the cost of controls expenditures.

So what are top performers doing right?

- Lines of business have established key risk indicators (KRIs) that predict and model risk assessment.
- Self-assessment and other reporting tools are standardized across the business.
- Controls have been optimized to improve effectiveness, reduce costs and support increased business performance.
- Key risk metrics have been established at the business level.

Enable risk management, communicate risk coverage

Making a move from being risk-averse to risk-ready may require a significant culture shift.

Organizations will want an executive champion to lead it, as well as tone-from-the-top support and executives who lead by example. Risk management is about changing the culture of the business. Organizations will want to communicate openly and often with all stakeholders. For greater assurance, organizations should provide stakeholders with independent, third-party verification.

Organizations also need to leverage their technology for maximum benefit. This does not mean risk initiatives should be technology-led. Rather, technology should be an enabler of change. Current Governance, risk management, and compliance (GRC) tools have the ability to enable an entire risk agenda.

However, organizations need to ensure that any risk-focused IT strategy aligns with broader risk and business strategies and the development of a Project Management Office (PMO) with quantitative managed objectives are established with portfolio and regulatory compliance tracking to achieve statistically analyzed processes.

So what are top performers doing right?

- Issue tracking, monitoring and reporting are regularly performed using GRC software.
- Risk dashboards are automated and include governance, risk and compliance indicators.
- Risk identification and assessment are regularly performed using GRC software.
- Internal and external audits.
- Organizational Risk Maturity survey assessments.

GRC FUNDAMENTAL COMPONENT: RISK ONTOLOGY

At the heart of GRC is adopting a coordinated, coherent approach to risk management across the organization, and core to that objective is developing and adopting a risk ontology.

What is Risk Ontology?

In the information sciences, ontology "formally represents knowledge as a set of concepts within a domain, and the relationships between those concepts. It can be used to reason about the entities within that domain, and may be used to describe the domain".

Some people think of ontologies as simply a nomenclature – but ontology is much more than a shared index, vocabulary or taxonomy.

A Risk Ontology, for example, would include a model with the definition of objects and concepts, and how they relate to one another. It would include rules about how concepts interact, and provide a basis for calculations and analytics. It would provide a basis for establishing consensus on the meaning of risk terms, and a model that explains their use.

Organizations manage risk by identifying it, analyzing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria – those concepts, and definitions of risk criteria – most importantly appetites, thresholds, rating schemes – can be part of a risk ontology shared by everyone.

Governance, Risk & Compliance (GRC)

What's in a Risk Framework?

Here are main things you want to get defined in a risk framework – this is a subset of the GRC Ontology; the core or 'engine' of risk management.

- Risk hierarchy; which includes Class and Type
- Mitigating Controls (and procedures)
- Risk Scores, and
- Metrics

Risks Scores (inherent and residual) will come as a by-product of assessments and can change.

Risk Framework: Five Easy Steps

Let's look at Five Easy (some may say not so easy…) steps to get started. Remember that core to GRC is adopting a coordinated, coherent approach to risk management across the organization, built on a common risk ontology. And, at the core of a risk ontology, is a ***risk framework***.

Quick review: Risk Frameworks provide risk management programs with better:

- **Coordination -** Provide a basis for coordinating risk across many activities in the organization.
- **Consistency -** Since all activities across the organization involve risk, a Risk Framework can be consistently applied to an entire organization, at its many functions, projects and activities.
- **Visibility** – While no single definition of risk exists, adoption of consistent concepts within a comprehensive framework can help the organization improve visibility into the true risk profile.
- **Governance** – Risk Frameworks can help the organization establish governance and manage risk more effectively, efficiently and coherently both internally and externally with 3rd parties.
- **Flexibility** – A Risk Framework, probably designed, can support variations of approaches, definition of threats and risk criteria across internal organization functions, partners and customers.
- **GRC Technology Platform Value** – Risk Frameworks are essential for driving value out of GRC technology platforms and enabling tools; they are only as good as the underlying frameworks, processes and procedures that define their use.

ENTERPRISE RISK MANAGEMENT (ERM)

In business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall. ERM can also be described as a risk-based approach to managing an enterprise, integrating concepts of internal control, Sarbanes–Oxley Act, and strategic planning.

ERM is evolving to address the needs of various stakeholders, who want to understand the broad spectrum of risks facing complex organizations to ensure they are appropriately managed. Regulators and debt rating agencies have increased their scrutiny on the risk management processes of companies. ERM frameworks suggest that base of effective system of governance and internal control is proactive, efficient and sustained ERM (refer to Chart 1).

The Framework of ERM can be summarized as follows:

- Establishing Context
- Identifying Risks
- Analyze/Quantify/Integrate Risks
- Prioritize Risk
- Treat/Exploit Risks
- Risk Assessment / Treatment

ERM Matrix Chart

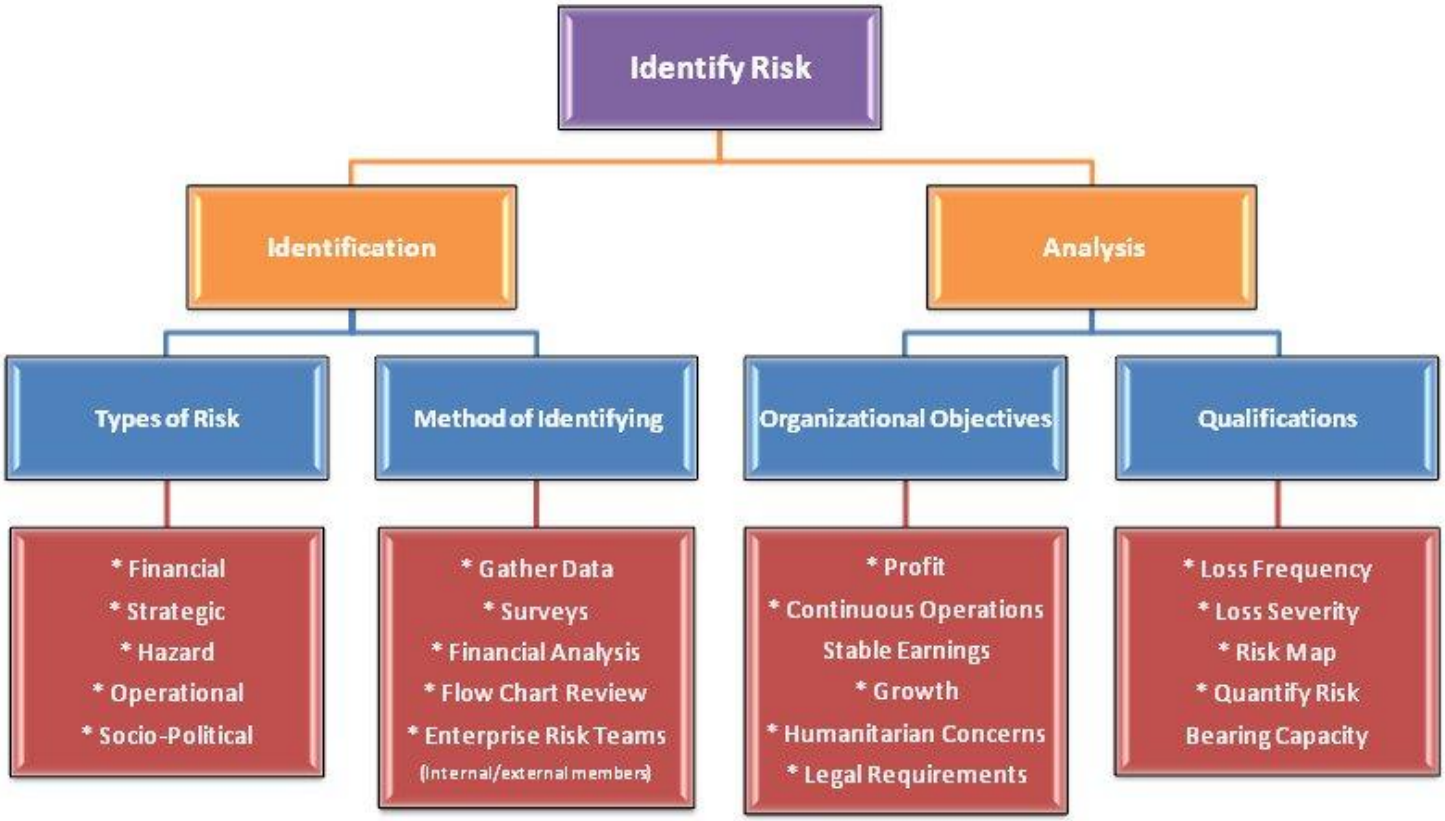


Chart 1 – Enterprise Risk Management Matrix

The RM Process

To sustain common, interoperable, and systematic approaches to risk management, organizations should employ a standardized risk management process.

This approach promotes comparability and a shared understanding of information and analysis in the decision process, and facilitates better structured and informed decision making. The organizational risk management process (refer to Chart 2) should be implemented while keeping in mind the previously articulated risk management principles.

The process is comprised of the following:

- *Defining and framing the context of decisions* and related goals and objectives;
- *Identifying the risks* associated with the goals and objectives;
- *Analyzing and assessing* the identified risks;
- *Developing alternative actions* for managing the risks and creating opportunities, and analyzing the costs and benefits of those alternatives;
- *Making a decision* among alternatives and *implementing that decision*; and

Chart 2 - Risk Management Process

- *Monitoring* the implemented decision and comparing observed and expected effects to help influence subsequent risk management alternatives and decisions.

Risk Communications

The foundation for each element of the risk management process is effective communications with stakeholders, partners, and customers. Consistent, two-way communication throughout the process helps ensure that the decision maker, analysts, and ultimately those charged to implement any decision share a common understanding of what the risk is and what factors may contribute to managing it. The concepts of uncertainty, perception, and tolerance for loss, which are intertwined with the concept of risk, should be accounted for as part of this communication.

Effective communication is also an essential element in executing adopted courses of action and in explaining risks and risk management decisions to external parties such as the public. Such external communications may occur throughout the risk management process and should be considered integral to effective risk management.

The organizational risk management process supports every mission of the organization and is generally compatible with other documented risk management processes. These include other risk management frameworks and standards promulgated by transnational organizations and other governments. Although it is

influenced by all of those approaches, this process is specifically designed for the totality of the organizational mission and is intended to be utilized to provide the organization with a standard process for risk management.

Elements of the Risk Management Process

Risk management supports a spectrum of organizational decisions, including strategic planning, standards and doctrine development, policy formulation, budget and resource allocation, program implementation, program evaluation and assessment, research and development investments, short-term operational activities, and problem-solving. The sections that follow describe all the steps in the application of the risk management process to support such decision making.

However, the realities of an organization's environment dictate that, at times, implementing the **six-step risk** management process may not be a linear progression. Program managers, operational personnel, analysts, and decision makers may be required to improvise and truncate steps in the process based on time and resource constraints. For example, to support operations such as law enforcement efforts and incident management activities, this risk management process are often executed in a less structured or expedited manner. In a tactical setting, such as law enforcement activities, circumstances may require that the decision cycle be completed in a matter of seconds. This is the reality of the organizational operating environment and the necessity that comes with reacting swiftly during times of stress.

Note that even when the risk management process is expedited or cannot be sequentially executed, it is still appropriate to continue through the cycle after a decision has been made to allow adjustments in execution and to better evaluate performance. You can also review my ERM Best Practices guide for 10 simple steps that may help you as you begin planning your ERM Plan. Review the **guide**.

The organizational risk management process consists of the following sequence of planning and analysis efforts:

1. Define the Context

To execute risk management, it is critical to define the context (*the circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood and assessed*) for the decision that the risk management effort will support. For complex problem-solving, an organization will typically assemble a risk analysis and management team (which are frequently referred to as a planning team, a task force, or a working group, among other descriptions) to help decision makers go through the risk management process.

When establishing the context, analysts must understand and document the associated requirements and constraints that will influence the decision making process, as well as key assumptions. While the analysis and management team members do not have to be risk experts, they must gain an understanding of the environment in which the risks are to be managed, taking into account political and policy concerns, mission needs, stakeholder interests, and risk tolerance. Defining the context will inform and shape successive stages of the risk management cycle.

It is important to set a context for ERM that enables an appropriate risk-reward balance. In other words, both a *defensive* stance of value protection (i.e. to minimize exposure to threats) and an *offensive* stance of value creation (i.e. to fully exploit opportunities).

Traditional approaches to risk management focus on value protection and pay only lip service to value creation. Their risk identification processes begin and end with the question "*What can hurt us?"* This tends to create a large list of risks, most of which are not significant to *enterprise* performance or viability.

One way to achieve a balance between the defensive and offensive stance is to begin the risk identification task by asking *"What do we want to achieve?"* followed by *"What drives uncertainty in the achievement of those objectives?"* or *"What could help or hinder us in the pursuit of our objectives?* It is essential to clearly articulate the organization's mission, goals, and objectives because they serve as the main point of reference for identifying and analyzing risks. A strong focus on objectives also helps to keep us connected to what is required for value creation.

The considerations for defining the context can be as complex and varied as the decisions they are intended to support. The following is intended to offer some structure in scoping the **variables to be considered** when executing the risk management process, although often times it is not feasible to study all of these factors:

1.1 Goals and Objectives

Ensure that the goals and objectives of the risk management effort align with the desired requirements, outcome, or end-state of the decision making process. Clearly defined goals and objectives are essential to identifying, assessing, and managing those areas that may threaten success.

1.2 Mission Space and Values

When defining the decision context, consider the mission space and values of the organization and its decision makers.

1.3 Policies and Standards

Ensure that risk management efforts complement and take into account any risk management policies, standards, or requirements the organization has in place.

1.4 Scope and Criticality of the Decision

Understand the decisions that have to be made, and the range of options available to leaders. The breadth and depth of the decisions' impact must also be considered. The risk analysis and management effort should be commensurate to that criticality.

1.5 Decision Makers and Stakeholders

Organizational leaders and their staff must be engaged at the outset of a risk management process so that the approach and presentation of results can be tailored to their preferences. It is also helpful to understand the authorities and responsibilities of leaders, as well as their comfort level with risk management concepts and language.

Similarly, stakeholders — those individuals or groups affected by the decisions — should be appropriately engaged and represented throughout the risk management process to ensure concerns are being addressed. This can be accomplished through direct interaction, such as conferences and public meetings.

1.6 Decision Timeframe

The timeframe in which a decision must be made and executed will dictate a number of the attributes of the risk management effort, including how much time is available for conducting formal analysis and decision review. Related to this issue is the frequency of the decision, which can also affect the risk management effort's analytic depth. The time horizon that the decision will impact must also be considered, such as whether the decision will have an influence only in the short-term or over a long period of time.

1.7 Risk Management Capabilities and Resources

At the beginning of the risk management process, it is useful to identify the staff, money, skill sets knowledge levels, and other resources available for risk analysis and management efforts. The implemented approach needs to be feasible and aligned with the organization's capabilities, capacity, and processes. Additionally, the resources applied to support the effort should be commensurate with the complexity of the issues involved and the magnitude of the decision. For example, it would be irresponsible to spend significant resources to support a decision with a minimal projected impact.

1.8 Risk Appetite

For far too long, risk professionals, coming from a value protection stance, have relied on using the magnitude of a risk as the sole criteria for deciding how much attention it merits. The logic goes like this: *Focus lots of effort on big risks and proportionally less effort on smaller risks*. The big problem with this approach is that it ignores the risk-reward relationship.

To help ensure consistent and appropriate risk-taking, an organization needs to articulate its appetite and tolerance for its principal enterprise risks. There is a lot of debate about the definition of risk appetite and risk tolerance. Here is how I define them:

- ***Risk Appetite*** refers to the level of threat exposure an organization is comfortable taking on in order to ensure it has ample opportunity to achieve its objectives.

- ***Risk Tolerance*** refers to the acceptable amount of variance around the targeted level of risk appetite.

1.9 Risk Tolerance Levels

Determining and understanding organizational decision makers' general risk tolerance level is helpful before embarking on the risk management process. Risk management efforts often involve tradeoffs between positive and negative outcomes. Having perspective on an organization or a decision maker's risk tolerance will help shape the assessments and the development of risk management alternatives that will be presented to leadership.

Articulating your risk appetite clarifies your comfort zone for the risk-return trade-off. Risk appetite and tolerance will vary depending on the set of threats and opportunities associated with a particular decision or strategy. For example, in some situations, we are willing to take big risks if they will help us to improve our performance or strategic positioning and if we believe that they can be managed appropriately. In other situations, we can't stomach even a small amount of risk, e.g., most organizations will invest a lot of resources into compliance activities, even if there is only a small risk that they might breach laws and regulations.

1.10 Availability and Quality of Information

When evaluating decision requirements, consider the availability and quality of information that can support the risk management effort, as available information will impact the design of the risk analysis approach. In engaging with decision makers at the outset of the risk management cycle, it is important to convey anticipated data limitations, including expected levels of uncertainty, so decision makers can adjust their expectations accordingly.

The ERM Design Approach

The above considerations shape and help define the design of the required processes to identify risks and conduct risk assessment and analysis and allow for the selection, implementation, and evaluation of risk management alternatives. By considering each of these elements systematically, decision makers and the analysts who support them are able to design an approach that is appropriate given the context.

Additionally, as the risk management process is iterative, the context may be redefined based on external events, shifting priorities, and new information. Considering such change is critical for ensuring that both the principles of flexibility and practicality are adhered to as part of risk management.

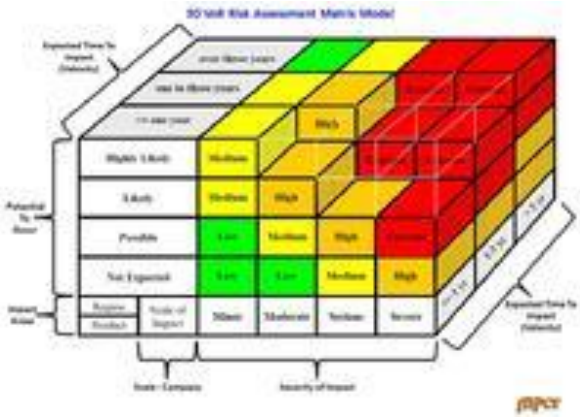
At the first stage of the ERM implementation cycle, it's essential to assess the organization's operating environment. While environmental scanning is a standard practice for strategic planning, many organizations don't yet use the results of the environmental scan to help them understand their enterprise risk management context.

The environmental scan you do for strategic planning can easily be expanded to identify the trends and risk factors that can have an impact on your organization's risk profile and on its preferred position on the risk-reward continuum. The ERM-oriented environmental scan gives a sense of the possibilities and potential limitations for both creating and protecting organizational value.

In recent years, it has become a risk management best practice to conduct an environmental scan prior to the annual risk profiling exercise. The trouble is, some drivers of risk can change rapidly and therefore should be monitored more frequently than once a year. One way to leverage the environmental scanning exercise is to distinguish between high velocity of risk (VoR) factors that can occur quickly with little or no warning (e.g. an earthquake, a disruptive technology) from risk factors with a lower velocity that can be foreseen (e.g. changes in employee demographics, seasonal variations).

The velocity of a risk factor is an important consideration in the development of effective risk detection strategies and risk treatment plans that occur in the ERM Implementation cycle.

For further details about utilizing VoR techniques go to section Enterprise Risk Modeling (page 37):



VoR Modeling concepts: **Read**

VoR concept was used to develop the first 3D VoR Modeling software by Michael McCormick. **Read**

2. Identify Potential Risk

For homeland security, there is a need to consider a wide variety of risks to support decision making. As previously noted, these considerations include strategic, operational, and institutional risks. The risks that are included in any particular assessment (sometimes called the assessment's scope) are largely determined by the decision the assessment is designed to inform. The decision context established in the previous step of the process should be used to determine what individual risks should be identified and assessed.

Identifying a preliminary list of risks can generally be done from a basic knowledge of the subject matter of the decision. To do so, it is sometimes helpful to think about the risks in terms of "risk to" and "risk from." This can be a very simple exercise of defining elements affected (goals, objectives, and systems) to determine the "risk to" and capturing the things (hazards, resources, and institutional failures) that impact them to determine the "risk from." This approach will yield a fairly broad list of potentially adverse outcomes that will assist in the identification of mitigation efforts and resources.

2.1 Unusual, Unlikely, and Emerging Risks

Prior to conducting a risk assessment, it is valuable to make a concerted effort to identify risks beyond those usually considered. For example, risks that are newly developing, even if they are poorly understood, are useful to identify. Risks that are highly unlikely but have high consequences should also be identified and incorporated into the assessment, if possible. This can even include identifying the risk of the unknown as a possible risk. Brainstorming is a common technique to identify these unusual, emerging, and rare risks. So, too, is involving a wide range of perspectives and strategic thinkers to avoid the trap of conventional wisdom and groupthink. Even when a risk is difficult to assess, it may still be important to try to understand and should be noted. It should also be acknowledged that no identification of risks is likely to capture every potential unwanted outcome — there will always be things that happen that are unanticipated.

2.2 Scenarios

It is generally appropriate and helpful for organizational risk assessments to use scenarios to divide the identified risks into separate pieces that can be assessed and analyzed individually. A **scenario** is a "hypothetical situation comprised of a hazard; an entity impacted by that hazard, and associated conditions including consequences when appropriate."

When developing scenarios to identify potential risks for a risk assessment, the set of scenarios should attempt to cover the full scope of the assessment to ensure that the decision maker is provided with complete information when making a decision. Also, the scenarios should not overlap, as including multiple scenarios that contain the same event may lead to double counting the risk.

Organizing the identified risks into a framework, such as with scenarios, is helpful preparation for creating a viable methodology in the next step in the risk management cycle. In addition, examining the risks in a structured way can also be used to identify gaps where potential risks have been left out.

3. Risk Assessments

The purpose of this step is to assess the identified risks and analyze the outputs of the assessment. This step consists of several tasks:

- Determining a methodology;
- Gathering data;
- Executing the methodology;
- Validating and verifying the data; and
- Analyzing the outputs.

In practice, these tasks, like the steps of the larger risk management cycle, rarely occur linearly. Instead, risk practitioners often move back and forth between the tasks, such as refining a methodology after some data has been gathered.

3.1 Methodology

When choosing a risk assessment methodology or framework, care should be given to remaining within the organization's capabilities.

The National Research Council notes *that "Rarely is there a single 'right' risk analysis tool, method or model to provide 'correct' analysis to support decision making. In general, a risk analysis is intended to combine data and modeling techniques with subject matter expertise in a logical fashion to yield outputs that differentiate among decision options and help the decision maker improve his or her decision over what could be accomplished merely with experience and intuition.*"

Methodology is used in this whitepaper to mean any logical process by which the inputs into an assessment are processed to produce the outputs that inform the decision. Methodology is defined as the systematic, theoretical analysis of the methods applied to a field of study. It comprises the theoretical analysis of the body of methods and principles associated with a branch of knowledge.

Likelihood is the chance of something happening, whether defined, measured or estimated in terms of general descriptors, frequencies, or probabilities.

Probability a risk is an event that "may" occur. The probability of it occurring can range anywhere from just above 0 percent to just below 100 percent (>0<100). (Note: It can't be exactly 100 percent, because then it would be a certainty, not a risk. And it can't be exactly 0 percent, or it wouldn't be a risk.)

Consequence, or impact, is the effect of an incident, event, or occurrence, whether direct or indirect. In organizational risk analysis, consequences include (but are not limited to) loss of life, injuries, economic impacts, psychological consequences, environmental degradation, and inability to execute essential missions.

There is no single methodology that is appropriate for measuring the likelihood and consequences of every organizational risk, and each methodology requires independent judgment regarding its design. In some cases, it may not even be necessary to explicitly determine likelihood and consequence.

3.2 Types of Methodologies

As a general rule, simple, but defensible, methodologies are preferred over more complicated methods. Simple methodologies are less prone to errors and are easier for stakeholders to understand. They are also more likely to fulfill the principles of transparency and practicality.

Organizational risk methodologies are often sorted into **qualitative** and **quantitative** categories, but when well-designed, both types of assessments have the potential to deliver useful analytic results. Similarly, both qualitative and quantitative methodologies can be needlessly complex or poorly designed. As stated previously, the methodology that best meets the decision maker's needs is generally the best choice, whether quantitative or qualitative.

- **Qualitative:** relating to, measuring, or measured by the quality of something rather than its quantity. (Merriam-*Webster Dictionary*)
- **Quantitative:** of or relating to how much there is of something : of or relating to the quantity or amount of something (Merriam-*Webster Dictionary*)
- **Qualitative risk assessment methodology:**

  Definition: set of methods, principles, or rules for assessing risk based on non-numerical categories or levels

  Sample Usage: The qualitative risk assessment methodology allows for categories of —low risk, —medium risk, and —high risk.
- **Quantitative risk assessment methodology:**

  Definition: set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment

  Sample Usage: Engineers at the plant used a quantitative risk assessment methodology to assess the risk of system failure.

  Annotation: While a semi-quantitative methodology also involves the use of numbers, only a purely quantitative methodology uses numbers in a way that allows for the consistent use of values outside the context of the assessment.

3.3 Collecting Data

Once a methodology for informing the decision has been determined, data must be gathered to populate the assessment. There are a number of potential sources for risk information. Some of the most commonly used sources for organizational risk assessments include historical records, models, simulations, and elicitations of subject matter experts.

When collecting data, attention should be paid to all aspects of the decision that are important, regardless of whether these aspects can be readily quantified. For example, when considering the consequences of

strategic organizational risks, the assessed consequences may include difficult-to-quantify psychological impacts in addition to consequences such as lives lost and economic damage. Structured techniques, such as value focused thinking, can help the analyst determine which aspects of consequences should be included in the methodology.

Many pieces of data are not known precisely. For example, the cost estimate for damage resulting from a major earthquake can be estimated by a subject matter expert to fall within a range, with some values being more likely than others. The assumptions and uncertainty in the inputs should be considered in each step of the assessment's methodology to determine how they affect the outputs. Uncertainty in the outputs should then be communicated to the decision maker, as well as the assumptions that underpin the analysis. It is also useful to consider the impact of the uncertainty and how sensitive the assessment of risk is to particular pieces of uncertain data.

3.4 Validation and Presentation

Throughout the process of executing the assessment, the gathered data and evidence should be carefully studied and compared to previous work — as should the results — as doing so is part of validation and verification.

Decision makers will rarely be well-served by only a simple presentation of the outputs of a risk assessment, so the data and evidence should be analyzed to identify relevant and interesting features to the decision maker. In a broad assessment, the decision maker will often have specific areas they are particularly interested in, and will ask the analysts to focus in on those areas. Follow-up analyses will then need to be completed. In this way, analysts will regularly iterate a cycle of analyzing risks and presenting the analysis to decision makers.

3.5 Integrating Alternatives

Often, the evaluation of alternative risk management actions is part of a risk assessment methodology. Though the development of alternatives is the next step in the risk management cycle, many organizational leaders prefer the alternatives to be integrated into the risk assessment, necessitating additional data collection and analysis. The earlier in the process the potential alternatives are known, the more efficiently their data collection can be integrated into the data collection for the rest of the assessment.

4. Develop Alternatives

In order to improve the organization's ability to prevent, protect against, respond to, recover from, and mitigate a variety of manmade and natural hazards, organizational leaders must focus their attention on identifying and executing actions to manage organizational risks. Ultimately, the objective of organizational risk analysis is to provide decision makers with a structured way to identify and choose risk management actions.

4.1 Identifying Options

Within the risk management process, the step of developing alternatives involves systematically identifying and assessing available risk management options. Portions of this step may be performed by different practitioners, but the alternatives development phase brings together proposed risk management actions with the results of a risk assessment, to include course-of-action comparisons.

This provides leaders with a clear picture of the risk management benefits of each proposed action or group of actions. The picture of potential benefits, when combined with an analysis of an action's costs — both monetary and non-monetary — can serve as a valuable resource for aiding decision makers in making effective and efficient organizational choices.

Ultimately, the development of alternative risk management actions should:

- Be understandable to participants of the process, including the decision makers and stakeholders;
- Match and comply with the organization's relevant doctrine, standards, and plans;
- Provide documentation with assumptions explicitly detailed;
- Allow for future refinements; and
- Include planning for assessment of progress toward achieving desired outcomes.

4.2 Risk Management Strategies

Risk management actions include strategies, treatments, or countermeasures for managing risks. Risks can be managed by one of four distinct methods: *risk acceptance, risk avoidance, risk control,* and *risk transfer*. For more information about these four risk management treatment options see ***section 8-Definitions***.

Table 2: Risk Methods Definitions

Risk Methods	Definition
Risk Acceptance	An explicit or implicit decision not to take an action that would affect a particular risk.
Risk Avoidance	A strategy or measure which effectively removes the exposure of an organization to a risk.
Risk Control/Reduction	A deliberate action taken to reduce a risk's potential for harm or maintains the risk at an acceptable level.
Risk Transfer/Deflection	Shifting some or all of the risk to another entity, asset, system, network, or geographic area.

For example, a decision may be made to not invest in a countermeasure because the cost outweighs the risk reduction return on investment. Responsible risk management dictates that for some risks the most appropriate action will be to do nothing and to accept the risk.

However, when the "no action" option is chosen, it should not be the result of inattention but of thoughtful analysis and careful consideration of the costs and benefits of alternative courses of action.

4.3 Methods for Alternatives

Developing and evaluating alternative courses of action involves both technical study and applied ingenuity. While approaches for developing and evaluating alternatives are as diverse as the problem sets, considerations may include:

- Reviewing lessons learned from relevant past incidents;
- Consulting subject matter experts, best practices and government guidelines;
- Brainstorming;
- Organizing risk management actions;
- Evaluating options for risk reduction and residual risk;
- Developing cost estimates for risk management actions;
- Comparing the benefit of each risk management action with its associated cost; and
- Eliminating potential options.

Evaluating risk management options should involve information generated in the context-setting and risk assessment steps of the risk management cycle. This information should be generated through analysis of the costs and other negative impacts, as well as the projected benefits of identified courses of action. It is important to note that risk management actions can be evaluated based on their potential to manage risk in the aggregate across a range of scenarios, as well as their ability to manage risks associated with a single scenario; maintaining both perspectives is crucial in identifying the most effective actions.

4.4 Requirements and Constraints

Alternatives development requires consideration of the needs and constraints of an organization during the decision making process. For example, the team developing alternatives must consider the time needed to implement each risk management option; the objectives of the option, methods to achieve the objectives, and the resources required to implement the option; performance objectives, measures, and targets; and the decision making environment that would influence strategy implementation and sustainability. In a sense, the developing alternatives step is about understanding and clearly communicating the costs and benefits, expected outcomes, and likelihood of success of each strategy option.

4.5 Iterative Process

Alternatives development should be treated as a process that is iterative and evolutionary. Since risks often shift, it is important to revisit the alternatives development process, incorporate new information, and re-evaluate the options based on changed circumstances. Changes in threats or the emergence of a new risk can make a previously discarded risk management option possible, or even preferable to other options.

5. Decide Upon and Implement Risk Management Strategies

Risk management entails making decisions about best options among a number of alternatives in an uncertain environment. The key moment in the execution of any risk management process is when a decision maker17 chooses among alternatives for managing risks, and makes the decision to implement the selected course of action. This can include making an affirmative decision to implement a new alternative, as well as the decision to maintain the status quo.

5.1 Presenting Information

For the “Decide and Implement” phase, decision makers need to consider the feasibility of implementing options, and how various alternatives affect and reduce risk. This includes the consideration of adequate resources, capabilities, time to implement, policy imperatives, legal issues, the potential impact on stakeholders, and the potential for creating new risks for the organization.

When providing decision makers with alternatives, analysts should present options, and their strengths and weaknesses, clearly and understandably in order to ensure that decisions are informed by a common understanding of the organization’s risks. Information should be tailored to the needs of leadership, and the risk analysis and management team should consider who the audience is when preparing to communicate assessments and strategies.

5.2 Document and Implement

Once a decision has been made, the decision maker must ensure that the decision is documented and communicated, and that an appropriate management structure is in place to implement the decision. Leadership should require comprehensive project management approaches that will document the planning, organizing, and managing of resources necessary for the successful implementation of the risk management strategy. This should include identifying metrics for the implementation process, which will allow the organization to track progress and improve future efforts. Additionally, leadership should develop an approach for the management of residual risk to the organization left after the decision.

6. Evaluation and Monitoring

This phase includes the evaluation and monitoring of performance to determine whether the implemented risk management options achieved the stated goals and objectives. In addition to assessing performance, organizations should guard against unintended adverse impacts, such as creating additional risk or failing to recognize changes in risk characteristics.

The evaluation phase is designed to bring a systematic, disciplined approach to assessing and improving the effectiveness of risk management program implementation. It is not just the implementation that needs to be evaluated and improved; it is the actual risk reduction measures themselves. Evaluation should be conducted in a way that is commensurate with both the level of risk and the scope of the mission.

6.1 Performance Measurement

Through effective evaluation and monitoring an organization may find it necessary to adjust its risk management options. It is crucial that a process of performance measurement be established to evaluate whether the actions taken ultimately achieved the intended performance objective. This is important not only in evaluating the success of the implemented option, but also in holding the organization accountable for progress.

A core element of evaluating and monitoring risk management options involves using effectiveness criteria to track and report on performance results with concrete, realistic metrics. In cases where the chosen course of action is to do nothing, the continued appropriateness of accepting the risk may be the best possible metric. In other cases, the best metric is often the reduction of the likelihood or consequences associated with a risk.

It is also important to monitor the larger context within which an identified risk and risk management effort exists. Good situational awareness may reveal changes in the context that require corresponding changes in the risk management effort. Both types of monitoring — effectiveness and situational awareness — are essential if risk management efforts are to be effective over time.

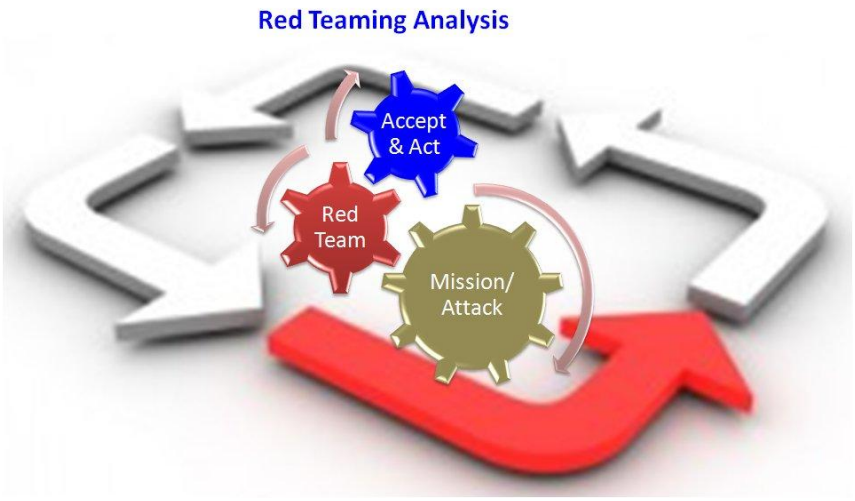
6.2 Logic Models

One way to develop measures that evaluate the implementation of a risk management decision is to build a performance logic model that defines causal relationships between activities and risk management goals. These logic models typically include:

- **Risk Management Goals:** A description of the overall end-state expected to be achieved in terms of managing identified risks.
- **Inputs:** A description of the resources that are used to carry out risk management efforts.
- **Efforts:** A description of the types of efforts or activities that, employing the inputs, work toward achieving the risk management goals.

- **Output:** A description of what is immediately produced by the activities, including metrics that can be used to measure that production.
- **Outcome Performance Measures:** A description of the combined effect that delivering outputs are expected to have, including measures that evaluate the impact of the combined efforts in achieving the risk management goals.

6.3 Models of Evaluation



Models of evaluation include red teaming (scenario role-playing), exercises, external review, and surveys. Different models of evaluation will require differing levels of involvement from organization leadership and staff. For example, red teaming and exercises should be guided by leadership and analysts. External review, however, is an independent activity that should not be influenced by the risk management activity under evaluation. Leadership must provide the appropriate and requested information to the external review team, and the process should be conducted in an independent and unbiased manner.

The benefit of testing effectiveness using these methods is that it provides different perspectives on the capabilities of the risk management program. It also allows one to validate what is going well, and areas that may need improvement.

Evaluating and monitoring implemented risk management strategies should be part of considering overall performance management of organizational activities.

Note: Read more on Red Team.

7. Risk Communications

Risk communication is the exchange of information with the goal of improving risk understanding, affecting risk perception, and/or equipping people or groups to take appropriate actions in response to an identified risk.

Communications underpins the entire risk management process. As explained earlier, organizational risk is a fluid concept affected by varying perceptions and loss tolerances, as well as uncertainty. As a result, it is essential that risks and risk management decisions are communicated between stakeholders, partners (external support), and customers. Communication requirements will differ, however, according to the audience and timeframe. Typically, risk communication is divided between internal and external audiences and between incident and standard timeframes.

Internal Risk Communications

Some risk communications are internal to an organization, such as that between analysts and decision makers. Maintaining two-way communication throughout the risk management process ensures that the key principles of risk management are met. For example, decision makers provide context (including values and perceptions) to bound analysts' exploration of risks and meet the organization's goals and objectives. Allowing decision makers input from the beginning of the process improves transparency, creates leadership buy-in, and sets the framework for an assessment tailored appropriately to the organization's needs and objectives. In turn, analysts provide information on risks and on possible actions to address the risks. Being transparent about methodology, limitations, and uncertainty provides decision makers with the most accurate, defensible, and practical information on which to base risk management decisions. Every internal stakeholder in the risk management process — decision makers, analysts, operational personnel, and program managers — should be included in the activities of that process through consistent, two-way communication.

External Risk Communications

The public and economy nature of organizational risk often necessitates that organizations communicate with external stakeholders, partners, and the public (where applicable). Risk management decisions should be communicated to the public (e.g. auto recalls) when appropriate in order to minimize fear while building trust. In addition, the government as well as the public and the private sector often have an important role to play in reducing risk (e.g. oil spills) and are therefore an integral part of the risk management process. When communicating to external parties, it is essential that varying risk perceptions and knowledge of risks be taken into account. Those outside the organization sometimes have a different perspective regarding risks than those within your organization, just as decision makers, analysts, operational personnel, and program managers have different perspectives from each other. Such differences mean that communications should be carefully tailored to the audience, but also represent an opportunity to strengthen the risk management process. External parties may help mold potential alternatives, provide context to the decision, and monitor and evaluate decisions that have been made. Thus external communications should also be two-way and should include an organization's public affairs professionals as appropriate.

Incident vs. Standard Timeframe Communications

How risk communications is defined and employed can differ based on a number of factors, including the relevance of time pressure, the purpose of the message, and the entity responsible for communicating the information. Standard types of risk communications involve little time pressure and are intended to empower decision making among partners, stakeholders and the public (if applicable).

Incident, or crisis, communications take place under different conditions than standard communications. In a crisis e.g. natural gas line explosion), empowering decision making remains a priority; however, time constraints are a critical consideration and the need to explain and persuade becomes increasingly important as a result of psychological changes in how people take in and act on information and protective guidance. Internal communications should remain bi-directional, but top-down decisiveness takes on greater importance. Externally, it is important that communications to stakeholders, partners, and the public provide clear information and, if appropriate, guidance on actions to take in a manner that is designed to minimize the anxiety that may arise in such a situation.

If the lines of communication have already been established under standard conditions, incident communications will occur more naturally and smoothly, ensuring that organization and its partners can more effectively prevent, protect, respond, and recover.

After an incident, standard communications should resume so that all stakeholders build a common understanding of what has happened, why certain decisions were made, and how to move forward. Essentially, an incident does not represent a break in the risk management process, but rather a temporary acceleration after which the process continues as normal.

Risk Communications Considerations

Risk communications will be most effective if guided by the following interrelated aims:

- **Plan for communications:** Communication efforts for decision makers and stakeholders need to be proactive as part of the risk management process; they should not be “tacked on” at the end as an afterthought. Furthermore, risk information needs to be readily available for relevant parties at all stages of the risk management cycle.

- **Maintain trust:** Past communication efforts give context to the organization’s next message, shaping how it will be received. Consistency is important, but only as long as it serves to build trust. When consistency is untenable in light of emerging information, then officials need to acknowledge it, including any errors that may be involved, and explain it. Once trust is lost, it is very difficult to recover (e.g. Enron scandal, October 2001)

- **Use language appropriate to the audience:** When communicating risk, it is important to consider the intended audience and tailor the language and channels used to effectively convey the information to promote and elicit the desired actions and outcomes.

- **Be both clear and transparent:** Clarity and transparency are important to effective communications. Clarity means communicating in a direct, simple and understandable way. Transparency in communications means disclosing assumptions, methodology, and uncertainty considered.

- **Respect the audience's concerns:** Risk communications are most effective when the recipient's concerns and/or issues are acknowledged. Maintaining open channels for collaboration or feedback fosters mutual understanding. Communicators should be both receptive and responsive to queries from decision makers and stakeholders.

- **Maintain integrity of information:** Effective risk communications should acknowledge uncertainty, note any limitations of information, make assumptions explicit, and distinguish assertions from judgments supported by analysis and evidence.

Communication connects each step of the risk management process. It is also crucial for linking the risk management principles and process. One cannot overstate the importance of risk communications in risk management.

ENTERPRISE RISK MODELING

Risk modeling refers to the models and methods used to evaluate risk and performance measures. Most organizations usually possess a simple financial model of their operations that describes how various inputs (i.e. risk factors, conditions, strategies and tactics) will influence the key performance indicators, which are used to manage the organization. Most of the structured financial models are deterministic models as they describe the expected outcomes from a given set of inputs without considering the probabilities of their outcome above or below the expected values and these models can be converted into stochastic models by treating certain inputs as variables.

There is a wide variety of risk modeling methods, which can be applied to a given task. They can be classified on the basis of the extent to which they rely on expert input as against availability of historical data. The classification can be given as below.

1. Methods which primarily rely on the availability of historical data
    a. Empirical distributions
    b. Regression
    c. Extreme value theory
    d. Stochastic differential equations

2. Methods which primarily rely on expert input rather than historical data
    a. Delphi method
    b. Influence diagrams

Sometimes the expert judgment is used to develop the logic of the model for supplementing the missing data besides the available data from the historic records.

3. The methods which rely on both the expert input and historical data
    a. Bayesian belief networks
    b. Fuzzy logic

These models are basically suited for the operational risk and the strategic risk.

Sometimes risks in the enterprise are related to each other. To predict the relationships which exist between two risks can be done through covariance matrix or through structural simulation of the model of an enterprise. As an example, using the economic scenario generation model, inflation rates and interest rates can be generated. The risk integration is also possible to analyze through structural simulation of the model. This allows a person to capture the dependencies among variable inputs in a simple, accurate and logically consistent way of the model's cause/effect linkages of these inputs to common higher-level inputs.

Risk mapping is done to prioritize risk according to frequency of risk, severity of risk or both. Risks in an enterprise can be monitored using risk dashboards, which is a graphical interface to represent the risks in an organization against their tolerance levels. Some of the measures required for the risk management can be

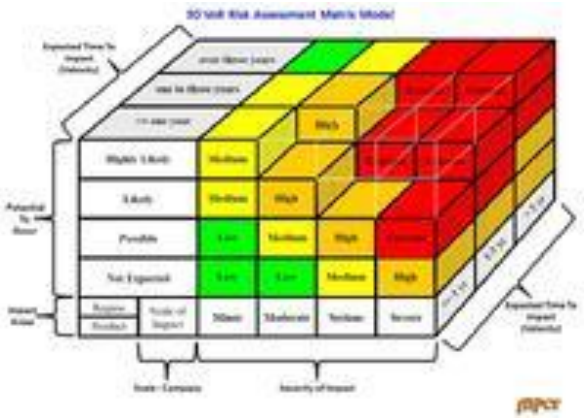
financial, human resources, marketing, underwriting, sales/distribution, investments, claims and other external data.

Thus, ERM is a properly structured and disciplined approach to managing risks. ERM aligns the strategies, processes, technologies and knowledge of an organization in order to ameliorate its ability to manage the uncertainties it faces. An enterprise wide risk management capability increases the risk sensitivity of the organization and decreases its functional barriers. Thus, ERM enhances the value of the organization as a whole.

VoR Modeling

The velocity of a risk factor is an important consideration in the development of effective risk detection strategies and risk treatment plans that occur in the ERM Implementation cycle.

Velocity of Risk (VoR) Concepts & Models



VoR Modeling concepts: **Read**

VoR concept was used to develop the first 3D VoR Modeling software by Michael McCormick. **Read**

Corporate Risk Modeling Tools

There is a verity of risk modeling tools on the market and they vary by organizational functional requirements from financial, human resource management to security modeling.

Below you can use these 3 free Excel tools that can be found on my website or direct download links below.

ERM Key Risks and Mitigation Plan Tool - Download

Corporate Compliance and Ethics Accountability Matrix Tool - Download

Corporate Risk Ranking Tool - Download

IN CLOSING

This document serves as set of guidelines to define the principles, process and operational practices of effective organizational risk management and is intended for organizations and personnel to adopt and employ. Applying consistent framework that promotes the understanding of sound risk management practices is a critical step toward creating a cohesive approach to risk management.

In order to promote and enhance the safety, security, and resilience of your organization, the organizational leaders and their organizational partners need to identify, understand, and develop strategies to prevent, mitigate, and control risks. The establishment and sustainment of a risk management culture across the organization and its partners will require continued commitment and attention from leadership and personnel. The development of risk management capabilities requires time, resources, training, and ongoing support by all levels of management. The organizational leadership must drive the train to lead the development and establishment of those capabilities to achieve an integrated approach to organizational risk management.

THE AUTHOR

Michael McCormick - Management Professional with 39 years of experience managing over $4 billion in PMOs, programs & projects for both the Commercial and Federal Government sectors and is a well known author, consultant, and authority on the subjects of Project Management Office (PMO), Risk Management (RM), Business Process Management (BPM), Project Portfolio Management (PPM), Construction Management (CM), Software Development and Technology Integration.

www.mccormickpcs.com