


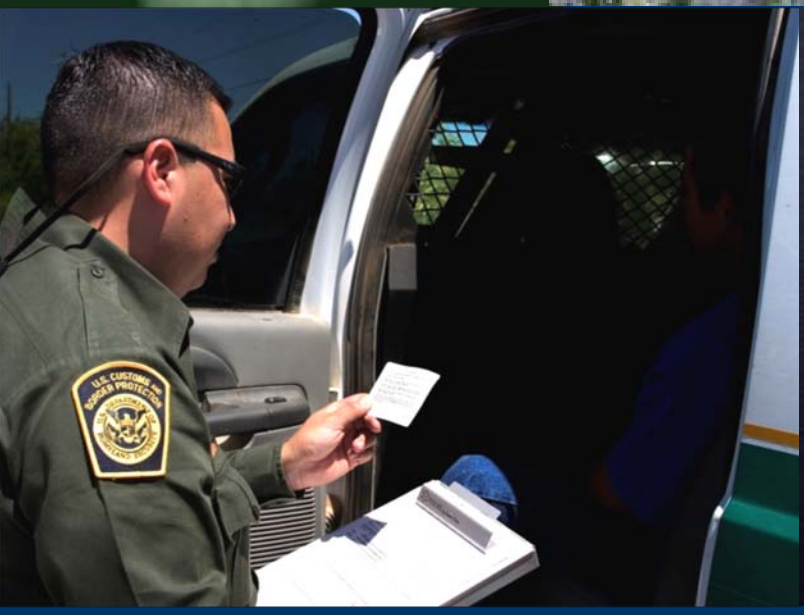


# Risk Management Fundamentals

Homeland Security Risk Management Doctrine

*April 2011*

Homeland Security

## *LETTER FROM THE UNDER SECRETARY*
## *NATIONAL PROTECTION AND PROGRAMS DIRECTORATE*

In May 2010, the Secretary of Homeland Security established a Policy for Integrated Risk Management (IRM). Central to this policy is the premise that security partners can most effectively manage risk by working together, and that management capabilities must be built, sustained, and integrated with Federal, state, local, tribal, territorial, nongovernmental, and private sector homeland security partners. While successful integration requires implementation across the entire homeland security enterprise, the Department of Homeland Security (DHS) plays an essential role in leading the unified effort to manage risks to the Nation from a diverse and complex set of hazards, including acts of terrorism, natural and manmade disasters, pandemics, cyber attacks, and transnational crime.

An essential first step in the integration of risk management is the establishment of doctrine and guidance. *Risk Management Fundamentals* is the first in a series of publications that will provide a structured approach for the distribution and employment of risk information and analysis efforts across the Department. While this is the capstone publication for homeland security risk management, implementation of risk management requires the combined efforts of Components to tailor and implement key risk management methods and practices. Homeland security risk management is on a positive trajectory and this publication will further enable DHS to mature and strengthen its capabilities to address homeland security risks. The key objectives of this publication are to promote a common understanding of and approach to risk management for homeland security; establish a common foundation that enables consistent risk management application and training; and support the development of a risk management culture and philosophy across DHS. *Risk Management Fundamentals* establishes doctrine for DHS, although concepts within the doctrine may be a useful guide to our Federal interagency partners, state and local agencies, as well as the larger homeland security community.

*Risk Management Fundamentals*, produced by the Office of Risk Management and Analysis, in coordination with the Office of Policy, has been vetted and approved by the DHS Risk Steering Committee, a governing body of which I serve as the Chairman. Pursuant to the authority vested in the Under Secretary for the National Protection and Programs Directorate by the Secretary of Homeland Security in Delegation Number 17001 to lead the Department's efforts to establish a common framework to address the overall management and analysis of homeland security risk, this publication is hereby recognized and approved for official use until revised or superseded.

RAND BEERS
UNDER SECRETARY
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
DEPARTMENT OF HOMELAND SECURITY

This page intentionally left blank.

# TABLE OF CONTENTS

This page intentionally left blank.

# I. KEY OBJECTIVES

This doctrine, *Risk Management Fundamentals*, serves as an authoritative statement regarding the principles and process of homeland security risk management and what they mean to homeland security planning and execution. It is intended as the capstone doctrine on risk management for the Department of Homeland Security (DHS). Furthermore, *Risk Management Fundamentals* serves as a foundational document supporting DHS risk management efforts in partnership with the homeland security enterprise.[1]

*Risk Management Fundamentals* is intended to help homeland security leaders, supporting staffs, program managers, analysts, and operational personnel develop a framework to make risk management an integral part of planning, preparing, and executing organizational missions. The development of homeland security risk management doctrine is an essential element in promoting a risk-informed culture enabling training, capability development, and integration across DHS to strengthen and improve the Nation's security. *Risk Management Fundamentals* articulates a desired end-state that DHS aspires to achieve in promoting risk management.

This doctrine is not a substitute for independent thought or innovation in applying these principles and concepts. Simply reading the doctrine will not make one adept in managing risks, nor will attempting to follow the ideas herein as if they were a checklist; rather, doctrine serves to shape how one thinks about the issues that you are considering and should be applied based on the operating environment. Homeland security practitioners should compare the doctrine herein against their own experience and think about why, when, and how it applies to their situation and area of responsibility.

## Purpose

The purpose of this document is to:

- Promote a common understanding of, and approach to, risk management;
- Establish organizational practices that should be followed by DHS Components;
- Provide a foundation for conducting risk assessments and evaluating risk management options;
- Set the doctrinal underpinning for institutionalizing a risk management culture through consistent application and training on risk management principles and practices; and
- Educate and inform homeland security stakeholders in risk management applications,

### A Note on the Scope and Application of this Document

*Risk Management Fundamentals* captures the theoretical underpinnings of homeland security risk management and articulates principles and practices that should be strived for across homeland security 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 homeland security decision making, applied in a variety of operating environments, many of which face constraints.

[1] As noted in the *2010 Quadrennial Homeland Security Review Report*, the homeland security enterprise "refers to the collective efforts and shared responsibilities of Federal, state, local, tribal, territorial, non-governmental, private volunteer, and private-sector partners — as well as individuals, families, and communities — to maintain critical homeland security capabilities. It connotes a broad-based community with a common interest in the safety and well being of America and American society."

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.

*Risk Management Fundamentals* may be helpful to Federal interagency partners, state and local agencies, as well as the larger homeland security community.

# II. INTRODUCTION

". . . a safe and secure homeland must mean more than preventing terrorist attacks from being carried out. It must also ensure that the liberties of all Americans are assured, privacy is protected, and the means by which we interchange with the world — through travel, lawful immigration, trade, commerce, and exchange — are secured. **Ultimately, homeland security is about effectively managing risks to the Nation's security."**

~ *Quadrennial Homeland Security Review* Report, 2010

## Homeland Security Risks

The United States homeland security environment is complex and filled with competing requirements, interests, and incentives that must be balanced and managed effectively to ensure the achievement of key national objectives. The safety, security, and resilience of the Nation are threatened by an array of hazards, including acts of terrorism, malicious activity in cyberspace, pandemics, manmade accidents, transnational crime, and natural disasters. At the same time, homeland security organizations must manage risks[2] associated with workforce management, acquisitions operations, and project costs. 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 government capabilities.

It is the role of DHS and its partners to understand and manage these myriad homeland security 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 American security. Compounding this complexity is the fact that future trends — such as technological advancements, global climate change, asymmetric threats, and the evolving nature of Nation-states — have the potential to significantly alter the homeland security 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 homeland security decisions.

"**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 actions taken."

*- DHS Risk Lexicon, 2010 Edition*

[2] Throughout this document, risk is defined as "the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences." *DHS Risk Lexicon, 2010 Edition.*

To improve decision making, leaders in DHS and their partners in the homeland security enterprise 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 homeland to make appropriate resource tradeoffs and align management approaches. Addressing these risks and promoting security is a shared responsibility that depends on unity of effort among Federal, state, local, tribal and territorial governments, the private sector, non-governmental organizations, and the citizenry as a whole.

## The Value of Risk Management

The Secretary of Homeland Security has established the requirement for DHS to build and promote an integrated approach to homeland security risk management, working with partners across the homeland security enterprise. The Department's role in establishing integrated risk management is to build security, safety, and resilience across domains by connecting efforts to prevent terrorism and enhance security, secure and manage our borders, enforce and administer our immigration laws, safeguard and secure cyberspace, ensure resilience to disasters, and provide essential support in assuring national and economic security.

Improved homeland security depends on connecting information about risks, activities, and capabilities and using this information to guide prevention, protection, response, and recovery efforts. The establishment of sound risk management practices across DHS and the homeland security enterprise will help protect and enhance national interests, conserve resources, and assist in avoiding or mitigating the effects of emerging or unknown risks. 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 preclude adverse events from occurring; however, it enables national homeland security efforts to focus on those things that are likely to bring the greatest harm, and employ approaches that are likely to mitigate or prevent those incidents. Furthermore, the American people, resources, economy, and way of life are bolstered and made more resilient by anticipating, communicating, and preparing for hazards, both internal and external, through comprehensive and deliberate 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. Establishing the infrastructure and organizational culture to support the execution of homeland security risk management is a critical requirement for achieving the Nation's security goals. Risk management is essential for homeland security leaders in prioritizing competing requirements and enabling comprehensive approaches to measure performance and detail progress.

### Resilience and Risk Management

One of the foundational concepts of homeland security is the need to build resilient systems, communities, and institutions that are robust, adaptable and have the capacity for rapid recovery. Resilience 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 disasters that do occur.

## Risk Management Applications

The practice of risk management allows for a systematic and comprehensive approach to homeland security decision making. Risk management promotes the development and use of risk analysis[3] to inform homeland security decision making, to better inform selection among alternative strategies and actions, and to evaluate the effectiveness of the activities we undertake. Risk management applications include:

### Strategic Planning

Homeland security 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. Homeland security 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, including grant funding. 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 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 homeland security 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.

[3] Risk analysis is the "systematic examination of the components and characteristics of risk." *DHS Risk Lexicon, 2010 Edition.*

This page intentionally left blank.

# III. HOMELAND SECURITY RISK MANAGEMENT TENETS AND PRINCIPLES

Risk management enables homeland security 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 homeland security risk management is neither feasible nor desirable, all DHS risk management programs should be based on two ***key tenets***:

- Risk management should enhance an organization's overall decision making process and maximize its ability to achieve its objectives.
- Risk management is used to shape and control risk, but cannot eliminate all risk.

The ***key principles*** for effective risk management include:

- Unity of Effort
- Transparency
- Adaptability
- Practicality
- Customization

A description of each principle follows:

***Unity of Effort:*** *The principal of unity of effort reiterates that homeland security risk management is an enterprise-wide process and should promote integration and synchronization with entities that share responsibility for managing risks*.

Risk management efforts should be coordinated and integrated among all partners, with shared or overlapping risk management responsibilities, to include Federal, state, local, tribal, and territorial governments, as well as the private sector, non-governmental organizations, and international partners. Most homeland security measures involve representatives of different organizations, 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 security challenges.

***Transparency:*** *The principle of transparency establishes that effective homeland security risk management depends on open and direct communications*.

Transparency is vitally important in homeland security 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 countermand the times when there is need for security of sensitive or classified information; however, it does suggest that the processes and methodologies used for homeland security 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.*

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

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

The limitations of managing homeland security risk arises from the dynamic nature of homeland security 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 a terrorist or criminal organization.

Homeland security decisions often are made amidst uncertainty, but that uncertainty does not preclude the need for sound 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:** The principle of customization emphasizes that risk management programs should be tailored to match the needs and culture of the organization, while being balanced with the specific decision environment they support.*

DHS 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.

# IV. A Comprehensive Approach to Risk Management

DHS decision makers should employ a comprehensive approach to understanding and managing risks so that they can enhance the quality of decisions throughout their organization[4] — thus supporting the DHS Policy for Integrated Risk Management.[5] 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 DHS 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 stewardship, personnel reliability, and systems reliability. Organizations across government and the private sector are all subject to these types of internal risks. 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, 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 homeland security 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."
>
> *- DHS Risk Lexicon, 2010 Edition*

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 homeland security risks, the categories in the following table help to define the landscape for an organization as it establishes a comprehensive approach to risk management. Identifying and understanding risks and their interactions ensures DHS leaders have a more complete perspective to manage risks and promote organizational effectiveness.

---

[4] Many organizations describe their comprehensive approach to risk management using the term **Enterprise Risk Management (ERM),** defined as "a comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization from achieving its objectives." *DHS Risk Lexicon, 2010 Edition.*

[5] The concept of Integrated Risk Management was defined in the DHS Secretary's Memorandum, *DHS Policy for Integrated Risk Management*, dated May 27, 2010.

**Organizational Risk Categories**

| | Strategic Risks | Operational Risks | Institutional 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.

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.

# V. THE HOMELAND SECURITY RISK MANAGEMENT PROCESS

To bolster common, interoperable, and systematic approaches to risk management, DHS organizations should employ a standardized risk management process.[6]

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 homeland security risk management process should be implemented while keeping in mind the previously articulated risk management principles.


**DHS Risk Management Process**

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
- *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.

[6] The homeland security risk management process was defined in the DHS Secretary's Memorandum, *DHS Policy for Integrated Risk Management*, dated May 27, 2010. This document incorporates and amplifies that risk management process.

### Risk Management Processes

The homeland security risk management process supports every mission of DHS and partner organizations 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.[7] Although it is influenced by all of those approaches, this process is specifically designed for the totality of the homeland security mission and is intended to be utilized to provide DHS with a standard process for risk management.

### Elements of the Homeland Security Risk Management Process

Risk management supports a spectrum of homeland security 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 is 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 homeland security 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.

The homeland security 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 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.

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**

[7] Examples of relevant international standards include the Australian and New Zealand Standard on Risk Management (AS/NZ 4360) and the International Organization for Standardization Principles and Risk Management Standard (ISO 31000).

**considered** when executing the risk management process, although often times it is not feasible to study all of these factors:

### 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.

### Mission Space and Values:

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

### 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.

### 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.

### 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.

### 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.

### 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.

### Risk Tolerance:

Determining and understanding the 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.

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.

### Designing an 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.

## 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.

### 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.

### Scenarios

It is generally appropriate and helpful for homeland security 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."
>
> *- DHS Risk Lexicon, 2010 Edition*

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. Assess and Analyze Risk

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.

### Methodology

When choosing a risk assessment methodology, care should be given to remaining within the organization's capabilities.[8]

[8] 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." Committee to Review the Department of Homeland Security's Approach to Risk Analysis, *Review of the Department of Homeland Security's Approach to Risk Analysis*, Washington DC, National Academies Press, 2010, p.94.

**"Methodology"** is used in this document to mean any logical process by which the inputs into an assessment are processed to produce the outputs that inform the decision.

The most important factor to consider in selecting a methodology is the decision the assessment must inform. The methodology should only be as complex as necessary to properly inform the decision.

In homeland security risk analysis, there are a large number of pre-existing methodologies that may be appropriately applied to similar decisions. However, some homeland security risk management decisions will require novel methodologies, as this is a new and quickly developing field. Hence, when trying to determine the methodology, assessments that have already been completed may be a good starting point but should not be considered as the only options. Though properly informing the decision is the prime factor when selecting a methodology, other concerns will also influence the choice. Data availability, as well as time, financial, and personnel constraints also play a role.

### Likelihood and Consequences

Homeland security risks can be assessed in terms of their likelihood and consequences.

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

**Consequence**, or impact, is the effect of an incident, event, or occurrence, whether direct or indirect. In homeland security 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.

*- DHS Risk Lexicon, 2010 Edition*

There is no single methodology that is appropriate for measuring the likelihood and consequences of every homeland security 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.

Many homeland security risk assessments consider homeland security risks as a function[9] of **Threats, Vulnerabilities, and Consequences (TVC)**. Explicitly considering each of the TVC factors is appropriate for many homeland security risks, such as those related to infrastructure protection.[10] However, considering TVC explicitly is sometimes not the best approach for other homeland security risk assessments — especially those that include institutional risks that can impact an organization's ability to meet operational and administrative requirements. In fact, one of the most common mistakes in homeland security risk analysis is misapplying the TVC framework. It is important that the TVC framework be applied only when appropriate to the subject matter of the analysis and the character of the assessed risks. In addition, analysts should be very careful when calculating risk by multiplying threats, vulnerabilities, and consequences, especially for terrorism, because interdependencies between the three

[9] "Function" means that a value is assigned to each input of threat, vulnerability, and consequence, and the inputs are considered in combination.

[10] The *National Infrastructure Protection Plan*, published in 2009, calls for infrastructure risks from any scenario to be considered "as a function of consequence, vulnerability, and threat." p. 32.

variables, and/or poorly executed mathematical operations, can lead to inaccurate results.[11]

### 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.

Homeland security risk methodologies are often sorted into **qualitative**[12] and **quantitative**[13] categories, but when well-designed, both types of assessments have the potential to deliver useful analytic results.[14] 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.

### Gathering 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 homeland security risk assessments include historical records, models, simulations, and elicitations of subject matter experts.

> **Elicitations** involve using structured questions to gather information from individuals with in-depth knowledge of specific areas or fields. They are typically used when the historical record is either nonexistent or is not appropriate for collecting data on a specific scenario.

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 homeland security 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 in California 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.

---

[11] As the National Academies of Science states: "The definition of Risk = T x V x C makes sense…but not for natural disasters." p. 99.

[12] Qualitative Risk Assessment methodology is defined as "a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels." *DHS Risk Lexicon, 2010 Edition.*

[13] Quantitative Risk Assessment methodology is defined as "a set of methods, principles, or rules for assessing risk based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment." *DHS Risk Lexicon, 2010 Edition.*

[14] The National Research Council notes that "narrative descriptions of non-quantitative information about risk are often as important to decision makers as is the more fully quantitative information." Committee to Review the Department of Homeland Security's Approach to Risk Analysis, *Review of the Department of Homeland Security's Approach to Risk Analysis*, Washington DC, National Academies Press, 2010, p.10.

### 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.

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

### Identifying and Assessing 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 homeland security 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.

## 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*.[15]

**Risk Management Strategies**

| | Definition |
|---|---|
| **Risk Acceptance** | An explicit or implicit decision not to take an action that would affect a particular risk.[16] |
| **Risk Avoidance** | A strategy or measure which effectively removes the exposure of an organization to a risk. |
| **Risk Control (or reduction)** | Deliberate actions taken to reduce a risk's potential for harm or maintain the risk at an acceptable level. |
| **Risk Transfer (or deflection)** | Shifting some or all of the risk to another entity, asset, system, network, or geographic area. |

## Methods for Developing and Evaluating 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;

[15] For more information about these four risk management treatment options see the *DHS Risk Lexicon, 2010 Edition.*

[16] 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.

- 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.

### Needs 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.

### 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 maker[17] 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.

### 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

[17] Within the homeland security enterprise, decision makers can be anyone from a national official to the head of a local law enforcement agency to a first responder.

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.

### 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.

### 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

### 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.

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.

### 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 homeland security activities.

## 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."
>
> *- DHS Risk Lexicon, 2010 Edition*

Communications underpin the entire risk management process. As explained earlier, homeland security risk is a fluid concept affected by varying perceptions and loss tolerances, as well as uncertainty. As a result, it is imperative that risks and risk management decisions are communicated between stakeholders, partners, 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 cross-agency nature of homeland security risk often necessitates that DHS communicate with external stakeholders, partners, and the public. Risk management decisions should be communicated to the public when appropriate in order to minimize fear while building trust. In addition, other forms of government as well as the public and the private sector often have an important role to play in reducing risk 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 Department sometimes have a different perspective regarding risks than those within the Department, 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. DHS communicates risks on a daily basis. Standard types of risk communications involve little time pressure and are intended to empower decision making among partners, stakeholders and the public.

Incident, or crisis, communications take place under different conditions than standard communications. In a crisis, 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 DHS and its partners can more effectively prevent, protect, respond, and recover. In addition, both the *National Response Framework* (January 2008) and the *National Incident Management System* (December 2008) call for a Communications Plan to be developed as one of the major components of establishing an Incident Command System and maintaining a common operating picture during an incident.[18]

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.

[18] For further information on incident communications requirements, see the *National Incident Management System published in December 2008,* which outlines incident communications on a more tactical level than explored in this document.

## 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.

- *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.

# VI. CONCLUSION

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

In order to promote and enhance the safety, security, and resilience of the Nation, DHS leaders and their homeland security partners need to identify, understand, and develop strategies to prevent, mitigate, and control risks. The establishment and sustainment of a risk management culture across DHS 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. DHS will continue to lead the development and establishment of those capabilities to achieve an integrated approach to homeland security risk management. In doing so, DHS will build on the foundation established by *Risk Management Fundamentals*.


Homeland Security