

DEVELOPING A RISK AND CRISIS COMMUNICATIONS PLAN

In order to function effectively during a crisis event, organizations must have a written plan that delineates the roles, responsibilities, key players, and procedures. The planning process and its eventual document will vary widely from one organization to another, as it needs to be based upon an internal needs assessment, the size of the organization, the severity and probability of likely crises, and other factors. The planning process traditionally begins with some type of formal, and preferably quantitative, risk assessment from which the written document is derived. This chapter will begin by providing a brief summary of the more common tools and techniques available for performing risk assessments and then delve more deeply into the content of a crisis communications plan (referred to hereafter as the "Plan"), including a discussion of planning guidelines, planning process suggestions, and key plan elements.

It should be noted that the Plan, as it is described in this chapter, is intended to focus solely on the communication process an organization undertakes when a crisis occurs. It does not detail the actual response of the organization to the crisis; that is more appropriately handled in a comprehensive crisis management plan. The Plan discussed here either functions as an element of the comprehensive crisis management plan or as a stand-alone document that is part of an organization's overall crisis response.

DEFINING ACCEPTABLE RISK

Prior to determining the proper tool for the organization's risk assessment process, consideration must first be given to how the idea of "acceptable risk" will be approached. This term and what flows from it has recently received substantial attention from the safety, health, and environmental (SH&E) professional community (Manuele 2008, 2009, 2010; Hansen 2008). In his writings on the subject, Manuele documents numerous standards and guidelines utilized worldwide that make frequent use of the term, yet his experience is that SH&E professionals are wary of using the term. He believes this occurs because of the limits of understanding the nature of risk, concern over subjective judgments made when risks are assessed, lack of statistical probabilities that allow risks to be numerically categorized, and lack of experience in significantly hazardous environments where "nontrivial" risks are accepted as part of daily operations.

For purposes of this chapter, the term "acceptable risk" is defined as: "That risk for which the probability of a hazard-related incident or exposure occurring and the severity of harm or damage that may result are as low as reasonably practicable and tolerable in the setting being considered" (Manuele 2009).

Hansen agrees and adds that acceptable risk will vary among and within organizations and must be evaluated within the context of what the audience views as acceptable. Further complicating this idea is the reality of opinions and attitudes: "Because attitudes about the acceptability of risks are not consistent, there are no universal norms for risk acceptability. What your stakeholders view as an acceptable risk will depend upon a number of factors" (Hansen 2008, p. 50).

Those factors include the following:

- Nature of the risk
- Who or what is at risk
- To what degree can the risk be controlled
- What is the risk taker's past experience

It is important to note that all four of those factors correspond closely to several of the 15 risk perception factors noted by Covello in the risk perception model described in Chapter 3. Figure 8.1 addresses the concept of acceptable risk to an audience.

RISK ASSESSMENT TOOLS SUMMARY

It is not the intention of this chapter to provide a comprehensive discussion of how to choose the appropriate risk assessment tool and then detail the process for its application, assessment, and implementation. The topic of risk assessment and the tools utilized in the process is extensive, and the reader is referred to numerous texts specific to the topic (Manuele 2008; Haight 2008; Covello 1993). Several of the risk assessment tools require fairly extensive expertise in order to properly apply and implement them, which may often be beyond the ability of internal organizational staff. In such cases, outsource

tion's risk assessment process, "acceptable risk" will be approached. Given substantial attention from the national community (Manuele 2008, subject, Manuele documents numerous make frequent use of the term, yet of using the term. He believes this ure of risk, concern over subjective istical probabilities that allow risks ce in significantly hazardous envi-art of daily operations.

able risk" is defined as: "That risk ent or exposure occurring and the low as reasonably practicable and 2009).

I vary among and within organiza-tion that the audience views as accept- opinions and attitudes: "Because stent, there are no universal norms as an acceptable risk will depend

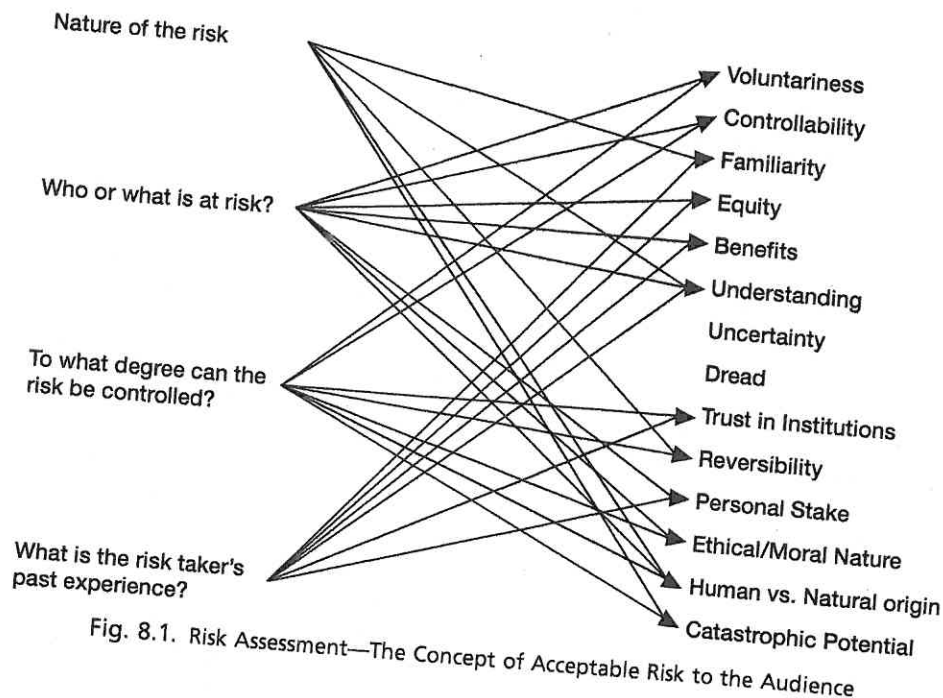


Fig. 8.1. Risk Assessment—The Concept of Acceptable Risk to the Audience

ing the risk assessment process may be the best alternative, depending upon the tool selected. In addition, the purpose of risk assessment in the development of a written risk and crisis communications plan is limited to helping the planning team understand what risks and crises are being addressed in the Plan in a fairly general manner. The list below provides a brief summary of three common risk assessment tools that can be utilized by the team crafting the written Plan (Hansen 2008; Manuele 2008). For a more detailed discussion of additional tools, the reader is referred to the sources quoted in this chapter.

1. **Checklists.** A checklist represents the simplest and most cost-effective method of risk assessment. It can be developed internally and requires little training to complete. The quality of the checklist developed is the variable that determines the effectiveness of its use and its eventual applicability, so a reasonable period of upfront development time is often necessary unless a prepared checklist is already available. The checklist format walks the organization through a set of defined criteria typically derived from published standards, codes, or industry best practices. The checklist is often in a question format with the appropriate answers being "yes," "no," or "not applicable," with a comments section for additional discussion.

Once completed, a checklist offers the organization a summary of the risks that exist, albeit with limited discussion about their severity and probability, except for what might appear in the comments section. Its value is the ease of development and the limited need for expertise in the method. The downside is

tors correspond closely to several the risk perception model described ceptable risk to an audience.

nprehensive discussion of how to detail the process for its applica-k assessment and the tools utilized to numerous texts specific to the several of the risk assessment tools apply and implement them, which onal staff. In such cases, outsourc-

that it takes some time upfront to develop and provides limited quantification of the risks.

2. **"What-if" checklist.** The strength of the checklist tool can be enhanced by combining it with a "what-if" process, the latter of which uses brainstorming sessions among organizational representatives to identify potential hazards, which are then transcribed to a checklist format. (It should also be noted that the "what-if" tool can be used independent of the checklist tool.) The use of a skilled facilitator helps this tool to be more comprehensive by helping the workgroup delve deeper into the potential hazards by asking "what if" repeatedly until the topic has exhausted possible hazards.

As with the use of a checklist technique, this is a tool that can be utilized with existing internal resources and limited formal training beyond helping the team members understand how to brainstorm.

3. **Matrices.** A matrix provides a method for analyzing a risk based upon two variables, typically severity and probability. It is a fairly easy tool to utilize internally with minimum expertise. The definitions for the variable vary greatly and can be customized to the organization's preference. Completion of a matrix simply requires the presence of those in the organization tasked with assessing risk. A facilitator can be chosen to help the group brainstorm about the various risks that may occur and the placement of them within the matrix. Once completed, the organization determines which of the risk categories it will focus on in terms of plan development and/or mitigation strategies. Typically not all risks are planned for; those with both low probability and severity may not provide a benefit in terms of time and monetary expenditures.

In Fig. 8.2, the variables are simply defined by terms "low," "medium," and "high." An organization would need to clarify internally how those terms applied and the use of a simpler matrix implies a greater degree of subjectivity on the part of those completing it.

In Fig. 8.3, the variables are defined in greater detail and an attempt is made to assign a numerical rating to the scale in order to increase the objectivity.

For a comprehensive treatment of the matrices approaches to risk assessment the reader is referred to the standard published by the U.S. Department of Defense (2002). Table 8.1 compares common risk assessment methods.

KEY PLANNING GUIDELINES AND PROCESSES

Before beginning the process of writing the Plan, an organization needs to ensure that it is prepared to implement several key planning guidelines and has a solid understanding of the purpose of the Plan. According to a planning document prepared and published by the Centers for Disease Control: "The plan is not a step-by-step 'how-to.' It is the bones of your work. It should systematically address all of the roles, lines of responsibility, and resources you are sure to encounter as you provide information to the public, media, and partners during a public health emergency. More than anything,

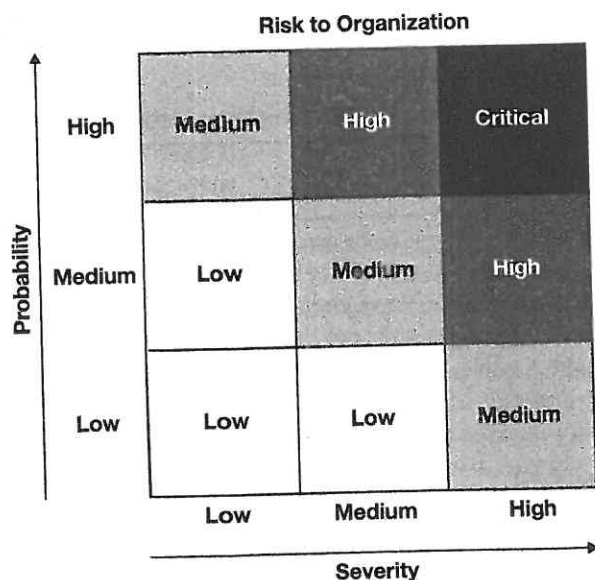


Fig. 8.2. Simple Risk Matrix

PROBABILITY										
Certain	10	20	30	40	50	60	70	80	90	100
Almost Certain	9	18	27	36	45	54	63	72	81	90
Very Likely	8	16	24	32	40	48	56	64	72	80
Probable	7	14	21	28	35	42	49	56	63	70
Likely	6	12	18	24	30	36	42	48	54	60
Likely	5	10	15	20	25	30	35	40	45	50
May Happen	4	8	12	16	20	24	28	32	36	40
Improbable	3	6	9	12	15	18	21	24	27	30
Unlikely	2	4	6	8	10	12	14	16	18	20
Very Unlikely	1	2	3	4	5	6	7	8	9	10
	Insignificant Injury	Minor Injury	Minor Injury	Illness - Injury	Illness - Injury	Major Injury	Major Injury	Single Fatality	Fatality	Multiple Fatalities
KEY										
Not Significant		0-3		May be ignored, no further action required						
Very Low		4-12								
Low		13-25		Ensure safe working						
Moderate		26-42		Refer to risk assesment, safe working procedures						
High		43-67		Monitor control measures						
Very High		68-100		Avoid if possible, full method statement if not						

Fig. 8.3. Risk Assessment Matrix with Weighted Values

TABLE 8.1. Comparison of Common Risk Assessment Methods

Method Type	Expertise Required to Apply	Benefits of Method/Results	Detriments of Results
Checklist	Minimal	• Can be completed someone with limited expertise • Provides a simple listing and brief understanding the risks a company is likely to encounter	• Quality of checklist determines quality of result • Provides limited analysis of the individual risk and no means to compare risks • Does not require input from various members of the organization
"What-if" checklist	Minimal	• Expands upon simple checklist and evaluates the various risks by imagining what would happen to the organization if they occurred • Can be completed within the expertise of the organization • Requires input from multiple organization members	• Quality of checklist determines quality of result • Provides limited analysis of the individual risk and no means to compare risks
Matrix	Minimal	• Can be completed within the expertise of the organization • Provides a simplified means of evaluating risks on the critical variables of severity and probability • Levels of quantification can be expanded by the team completing the matrix • Can be used to compare and contrast various risks	• Does not require input from various members of the organization • Comparison of risks is limited to review of two variables

your crisis communications plan is your resources of information—the 'go-to' plan for must-have information" (Reynolds 2002, p. 69).

While each organization's written planning documents for emergency and crisis responses will vary, the Plan will generally fit into the overall framework in one of two ways: either it exists as a stand-alone document and is cross-referenced to other emergency plans, or is a separate element within an organization's overall crisis management plan. Both formats work and neither has any particular benefits. The content is w

defines and differentiates a high-quality Plan, as does the accessibility of the Plan by those who need it when they need it.

As noted above, the Plan needs to begin with some type of risk assessment that defines what types of risks and crises the Plan will cover. This information belongs at the very beginning of the Plan and will be addressed in greater detail later in the section that discusses plan elements. The Plan also needs to have management support in place before the development process begins. This support takes several forms, the first of which is a written and verbal commitment from the highest executive in the organization about the importance of the Plan and the process to develop it. Management support also takes the form of dedicating staff time to develop the Plan and ensuring there are financial resources available to implement it. This commitment will vary among different organizations but is essential before moving forward. Any planning process that begins without it will most assuredly be wasted time and will produce a document that is never used except when needed to document simply that it exists.

As noted above by Reynolds, crisis communications plans are intended to be utilized during a crisis, which necessitates that they are dynamic and minimalist documents that provide general direction. The document must be the authority for crisis team members, provide a summary of important information, and guide their activities during the crisis event, rather than a detailed approach to crisis management. Since each crisis is different and progresses along paths that may not be easily controlled, providing an outline for the team to follow serves its purposes better than a set of length and detailed policies and procedures.

In addition to being a dynamic document during its use, the Plan must also be developed with the understanding that it will need ongoing review and revision if it continues to be a helpful tool for the crisis team. Regular reviews that are planned for both in terms of timing and resources are critical and should occur at timeframes of no less than annually. Other situations that would necessitate a review would be following a crisis that is part of a "lessons learned" review and any major change in the organizational structure or operations. In order to ensure that the organizational changes are accounted for in the Plan, it is a good idea to assign a staff person the task of a regular paper review, perhaps as often as monthly. This regular review results in notifying others only when changes are necessary and convenes the entire planning team only when needed.

It is also critical to note that the Plan should be a controlled document, with additions and revisions made through a formally documented process that allows for tracking and a means to ensure that only the most recent versions are available for general review. Internal staff must be informed that making and distributing copies of the document is limited to one identified staff person or department. Distribution outside of the organization also needs to occur only through channels that are delineated in the Plan. This is not to suggest that the Plan is a confidential, top-secret document, but because of the nature of the activities detailed within it, ensuring that only the most recent document is distributed within and outside of the organization serves to reduce confusion when the Plan needs to be implemented.

Once the management support and direction has been established, a planning team needs to be gathered and tasked. Again, each organization brings a variety of

representatives to the process and will vary in the number and expertise of the team members. At the very least, team members should represent key departments such as executive management, human resources, SH&E, and public relations. Other internal members should come from production/operations and internal emergency response teams, if appropriate. Depending upon the level of internal expertise, outside consultants with crisis planning expertise may be called upon to either be planning team members or perhaps even lead the effort. In the latter scenario, it is critical that the external consultants be able to "hand off" the document to operational staff once it is completed, unless the organization expects the external consultants to be a part of the response. If not, the internal staff needs to be able to implement the Plan, literally at a moment's notice.

Lastly, before the Plan can be drafted, more than just management support and risk assessment information needs to be available to the team. Data gathering can be a team task or can be done prior to the first meeting but at the very least team will need to know some of the following:

- Designated staff members (line and management) by title and department of who will be responsible for the actual response.
- Other emergency and crisis plans that exist within the organization and how this Plan will fit into the existing structure.
- What processes are already in place within the organization to determine which information can be disseminated, by whom, and to whom.
- The names of those members of the organization permitted to perform the role of spokesperson and public information officer.
- Representatives from other emergency response organizations who are expected to be part of the Plan team.
- A copy of existing mutual aid agreements (MAE) or memorandums of understanding (MOU) with other local emergency response organizations.
- Any other document, policies, or programs that currently exist that will need to be reviewed and incorporated into the Plan. These would include any prepared key messages. If none are available, the team needs to know if they will be responsible for developing them.
- A list of the audiences expected to be impacted by the implementation of the Plan and existing lines of communication with each audience.
- The resources and facilities that will be available to the team during the implementation of the Plan and the means of securing them.
- Information regarding any pre-training that might be helpful to the Plan team members so that they may function more effectively in their roles.

Not all of the details for each of the points above may be known at the time the team begins to develop the Plan. Some will become part of the information gathering process.

KEY PLAN ELEMENTS

Prior to the actual work of developing the Plan, the goals for the process and product should be established. As noted above, these goals ought to originate within the management of the organization so that the final Plan can be approved and continue to receive the support needed. Most Plans have at least two major goals: to anticipate and prevent crisis when possible, and to respond to crises effectively by providing timely, accurate, and helpful information to identified publics (Reynolds 2002). Beyond these major goals, individual needs of the organization can be addressed.

Numerous formats exist for the outline of the Plan (Fearn-Banks 2007; Lundgren and McMakin 2004; Reynolds 2002). A review of several formats reveals many common elements and few differences. Each organization should undertake a review of several formats before deciding on the one that works for its needs. In addition, any of the formats can be modified to meet unique planning needs or situations; using them as boilerplates helps ensure that key information and content is not missed.

The following Plan outline represents a culling of several formats and presents the best overall outline that will address the needs of most organizations (Reynolds 2002; Lundgren and McMakin 2004; Fearn-Banks 2007):

- **Title page.** This page should include some reference to the initial approval date of the Plan as well as the current version and its associated approval date. This page may also include a summary of all Plan reviews/revisions and their associated dates or this information may be listed elsewhere in the Plan. As noted above, the organization should also maintain a log of the various revisions, noting the changes in summary form. This log does not necessarily need to be part of the Plan but should be referenced somewhere and should be readily available for review. Finally, the signature of the key executive approving the Plan should appear at the bottom of the title page. Alternatively, a good way to demonstrate the organization's support for the Plan is to follow the title page with a brief statement from the key executive detailing the importance of the Plan and its association with the organization's overall mission statement, followed by a signature and date.
- **Authority.** This section is a comprehensive list of all regulatory and statutory requirements that affect the organization and require the development of the Plan.
- **Purpose.** This section answers the question of what the Plan is intended to do, for, and by whom. This section should also include a brief statement of the management support of the Plan and how it fits into the organization's overall mission (if not addressed on a separate page as noted above). It can also detail the philosophical position the organization takes with regard to crisis communications.
- **Scope.** This section provides a list and/or description of what is covered by the Plan. This should be a listing of the specific crisis events that are covered, as well as what parts of the organization may need to participate in the implementation.

- **Situations and assumptions.** This section addresses the planning environment and the circumstances under which crises may arise that are covered by the Plan. It also describes how a crisis is identified by internal members of the organization, when the Plan is activated, and what resources are available for each of the crisis events covered.
- **Audience profile.** This section details the different audiences for which the Plan was developed, delineated by specific crisis if needed, and should provide a basic description of each of the audience's characteristics.
- **Concept of operations.** This section describes the general plan of action during a response and makes up the critical functionality of the Plan. Organizational chains of command are identified here as well as the method by which the Plan is activated. Crucial approval processes for what, how, and when communications may occur need to be detailed here. Some Plans use this space to identify the process by which partnership activities are initiated and/or how the organization might begin to become involved in a public response and participation in an emergency operations command center.
- **Key communication strategies.** This section details the methods of communication that will occur both internally and externally and how those channels might be accessed.
- **Organization and assignment of responsibilities.** This section addresses the delegation of responsibilities. This includes the Plan's participants, the designation of a lead spokesperson and additional spokespeople if needed, how 24/7 staffing will be ensured, how to ensure that news is properly disseminated, and how interagency activities will begin to occur. Finally, this section often details, by organization and title, other participants in the response. For ease of understanding, a flow chart or table of organization can be utilized in large, more complex organizations to clearly delineate lines of authority and relationships between all of the key parties.
- **Evaluation of the communication efforts.** An organization should identify in advance how it intends to evaluate the success of the communication activities when the Plan is implemented so that a method for data gathering can also begin upon implementation of the Plan. This section should detail critical data points. Note that this section is differentiated from the following one in that it collects data for predetermined evaluation measures that will be used both during the Plan implementation as well as after. The information gathered will also be used for Plan development and maintenance, as described in the next category.
- **Plan development and maintenance.** This section provides details on when and how the Plan will be reviewed and updated, including the circumstances under which the reviews will occur. It should also address the methods for controlling the distribution of the document and the method for tracking the reviews through some type of log or similar document.
- **Appendixes.** While the text of the Plan is the working document and should be brief and user-friendly, additional information to be used as references during

implementation need to be readily available and literally attached to the Plan. Some of the more common appendixes include:

- Logistical details
- Call down lists
- Available materials
- Location of prepared key messages (message maps)
- News conference guidelines*
- Media relations reminders*
- Equipment, supplies, and services

*The reader is referred to Chapter 7 for a more detailed discussion of the development of a media communications plan.

REFERENCES

- Covello, V.T. and M.W. Merkhoher. 1993. *Risk Assessment Methods: Approaches for Assessing Health and Environmental Risks*. New York: Plenum Press.
- Fearn-Banks, K. 2007. *Crisis Communications: A Casebook Approach*, 3rd ed. Mahwah, New Jersey: Lawrence Erlbaum Associates.
- Haight, J.M., ed. 2008. *The Safety Professionals Handbook: Technical Applications*. Des Plaines, IL: The American Society of Safety Engineers.
- Hansen, M. 2008. "Applied Science and Engineering: Systems and Process Safety." In *The Safety Professionals Handbook: Technical Applications*, edited by J.M. Haight. Des Plaines: IL: The American Society of Safety Engineers, pp. 37-69.
- Lundgren, R.E. and A.H. McMakin, A.H. 2004. *Risk Communication: A Handbook for Communicating Environmental, Safety, and Health Risks*, 3rd ed. Columbus, OH: Battelle Press.
- Manuele, F. 2008. *Advanced Safety Management*. Hoboken, NJ: John Wiley & Sons, Inc.
- Manuele, F. 2009. "Prevention Through Design: Guidelines for Addressing Occupational Risks in Design and Redesign Processes." Technical publication TR-Z790.001. American Society of Safety Engineers, Des Plaines, IL.
- Manuele, F. 2010. "Acceptable Risk." *Professional Safety* 55(5):30-38.
- Reynolds, B. 2002. "Crisis and Emergency Risk Communication." U.S. Centers for Disease Control and Prevention, Atlanta, GA.
- U.S. Department of Defense. 2002. "Standard Practice for System Safety." MIL-STD-882D and E. Washington D.C. Also available online at <https://acc.dau.mil/CommunityBrowser.aspx?id=255833>