First Responders Handbook
An Introduction
Michael L. Madigan

Threat/vulnerability assessments and risk analysis

Publication details
Michael L. Madigan
Published online on: 07 Sep 2017

Accessed on: 02 Jan 2019

PLEASE SCROLL DOWN FOR DOCUMENT

Full terms and conditions of use: https://www.routledgehandbooks.com/legal-notices/terms

This Document PDF may be used for research, teaching and private study purposes. Any substantial or systematic reproductions, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The publisher shall not be liable for an loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
Introduction

There are fundamental principles underlying the threat-assessment approach. The first principle is that targeted violence is the result of an understandable and often discernible process of thinking and behavior. Acts of targeted violence are neither impulsive nor spontaneous. Ideas about monitoring an attack usually develop over a considerable period of time. In targeted violence, the subject must engage in planning around a series of critical factors such as which target(s) to select, the proper time and approach, and the means for violence.

A potential attacker may collect information about the target, the setting of the attack, or about similar attacks. He or she may communicate ideas to others. For some of these individuals the process of planning and thinking about the attack dominates their lives and provides a sense of purpose or an attainable goal by which they see an end to their emotional pain.

The second principle is that violence stems from an interaction between the potential attacker, past stressful events, a current situation, and the target. As noted above in the discussion of the risk-assessment model, researchers and practitioners are moving away from exclusive focus on the individual and toward a more situational/contextual understanding of risk.

An assessment of the attacker may consider relevant risk factors, development and evolution of ideas concerning the attack, preparatory behaviors, and an appraisal of how the individual has dealt with unbearable stress in the past. When usual coping mechanisms are ineffective, people often react by becoming physically ill, psychotic, self-destructive, or violent toward others. It is useful to consider how the potential attacker has responded in the past when stressful events overwhelmed his/her coping resources.

An assessment of the risk may be informed by an examination of the person’s history of response to traumatic major changes or losses, such as loss of a loved one (e.g., ending of an intimate relationship or loss of a
parent) or loss of status (e.g., public humiliation, failure, or rejection, or loss of job or financial status). The salience of the risk may be determined by examining the types of event that have led the individual to experience life as unbearably stressful, the response to those events, and the likelihood that they may recur.

In addition to assessing the potential attacker and past stressful events, the evaluator must also appraise the current situation and the target. Consideration of the current situation includes both an appraisal of the likelihood that past life events which triggered consideration of self-destructive or violent behavior will recur (or are recurring) and an assessment of how others in the subject’s environment are responding to his/her perceived stress and potential risk.

Since others may act to prevent violence, it is useful to know whether people around the subject support, accept, or ignore the threat of violence, or whether they express disapproval and communicate that violence is an impermissible and unacceptable solution to the problem. Finally, an evaluator must assess relevant factors about the intended target, including the subject’s degree of familiarity with the target’s work and lifestyle patterns, the target’s vulnerability, and the target’s sophistication about the need for caution.

The third principle is that a key to investigation and resolution of threats is that those who commit acts of targeted violence often engage in discrete behaviors that precede and are linked to their attacks, including thinking, planning, and logistical preparations.

Attack-related behaviors may move along a continuum beginning with the development of an idea about an attack, moving to communication of these ideas or an inappropriate interest in others, to following, approaching, and visiting the target or scene of the attack, even with lethal means. Learning about and analyzing these behaviors may be critical to an appraisal of risk.

**Threat assessment**

The first step in a risk-management program is a threat assessment. A threat assessment considers the full spectrum of threats (i.e., natural, criminal, terrorist, accidental, etc.) for a given facility/location. The assessment should examine supporting information to evaluate the likelihood of occurrence for each threat. For natural threats, historical data concerning frequency of occurrence for given natural disasters such as tornadoes, hurricanes, floods, fire, or earthquakes can be used to determine the credibility of the given threat.

For criminal threats, the crime rates in the surrounding area provide a good indicator of the type of criminal activity that may threaten the facility. In addition, the type of assets and/or activity located in the
facility may also increase the target’s attractiveness in the eyes of the aggressor. The type of assets and/or activity located in the facility will also relate directly to the likelihood of various types of accidents. For example, a facility that utilizes heavy industrial machinery will be at higher risk for serious or life-threatening job-related accidents than a typical office building.

**Vulnerability assessment**

Once the credible threats are identified, a vulnerability assessment must be performed. The vulnerability assessment considers the potential loss from a successful attack as well as the vulnerability of the facility/location to an attack. Impact of loss is the degree to which the mission of the agency is impaired by a successful attack from the given threat.

A key component of the vulnerability assessment is properly defining the ratings for impact of loss and vulnerability. These definitions may vary greatly from facility to facility. For example, the amount of time that mission capability is impaired is an important part of impact of loss. If the facility being assessed is an air route traffic control tower, a downtime of a few minutes may be a serious impact of loss, while for a social security office a downtime of a few minutes would be have a minor impact. A sample set of definitions for impact of loss is provided below. These definitions are for an organization that generates revenue by serving the public.

- **Devastating**: The facility is damaged and contaminated beyond habitable use. Most items/assets are lost, destroyed, or damaged beyond repair/restore. The number of visitors to other facilities in the organization may be reduced by up to 75% for a limited period of time.
- **Severe**: The facility is partially damaged and contaminated. Examples include partial structure breach resulting in weather/water, smoke, impact, or fire damage to some areas. Some items/assets in the facility are damaged beyond repair, but the facility remains mostly intact. The entire facility may be closed for a period of up to two weeks and a portion of the facility may be closed for an extended period of time (more than one month). Some assets may need to be moved to remote locations to protect them from environmental damage. The number of visitors to the facility and others in the organization may be reduced by up to 50% for a limited period of time.
- **Noticeable**: The facility is temporarily closed or unable to operate, but can continue without an interruption of more than one day. A limited number of assets may be damaged, but the majority of the facility is not affected.
• The number of visitors to the facility and others in the organization may be reduced by up to 25% for a limited period of time.
• Minor: The facility experiences no significant impact on operations (downtime is less than four hours) and there is no loss of major assets.

Vulnerability is defined to be a combination of the attractiveness of a facility as a target and the level of deterrence and/or defense provided by the existing countermeasures. Target attractiveness is a measure of the asset or facility in the eyes of an aggressor and is influenced by the function and/or symbolic importance of the facility. Sample definitions for vulnerability ratings follow.

• Very high: This is a high-profile facility that provides a very attractive target for potential adversaries, and the level of deterrence and/or defense provided by the existing countermeasures is inadequate.
• High: This is a high-profile regional facility or a moderate-profile national facility that provides an attractive target and/or the level of deterrence and/or defense provided by the existing countermeasures is inadequate.
• Moderate: This is a moderate-profile facility (not well known outside the local area or region) that provides a potential target and/or the level of deterrence and/or defense provided by the existing countermeasures is marginally adequate.
• Low: This is not a high-profile facility and provides a possible target and/or the level of deterrence and/or defense provided by the existing countermeasures is adequate.

The vulnerability assessment may also include detailed analysis of the potential impact of loss from an explosive, chemical, or biological attack. Professionals with specific training and experience in these areas are required to perform these detailed analyses. A sample of the type of output that can be generated by a detailed explosive analysis is shown in Figure 3.1. This graphic representation of the potential damage to a facility from an explosive attack allows a building owner to quickly interpret the results of the analysis, although a more fully detailed and quantitative engineering response would be required to design a retrofit upgrade. In addition, similar representations can be used to depict the response of an upgraded facility to the same explosive threat.

This allows a building owner to interpret the potential benefit that can be achieved by implementing various structural upgrades to the building frame, wall, roof, and/or windows (Figure 3.2).
Chapter three: Threat/vulnerability assessments and risk analysis

Risk analysis

A combination of the impact of loss rating and the vulnerability rating can be used to evaluate the potential risk to the facility from a given threat. Flowchart depicting the basic risk-assessment process (Figure 3.1): this is just one of many types of flowcharts, the type used will vary depending on one’s needs.

Upgrade recommendations

Based on the findings from the risk analysis, the next step in the process is to identify countermeasure upgrades that will lower the various levels of risk.

If minimum standard countermeasures for a given facility level are not currently present, these countermeasures should automatically be included in the upgrade recommendations. Additional countermeasure upgrades above the minimum standards should be recommended as necessary to address the specific threats identified for the facility.

Flowchart depicting the basic risk-assessment process; this is just one of many types of flow charts. This is just an example, and it will vary depending on one’s needs (Figure 3.2).
The estimated capital cost of implementing the recommended countermeasures is usually provided in the threat/vulnerability assessment report. The estimated installation and operating costs for the recommended countermeasures are also usually provided in the threat/vulnerability assessment report. All operating costs are customarily estimated on a per year basis.

Figure 3.2 Security risk management.
Chapter three: Threat/vulnerability assessments and risk analysis

Re-evaluation of risks

The implementation of the recommended security and/or structural upgrades should have a positive effect on the impact of loss and/or the vulnerability ratings for each threat. The final step in the process is to re-evaluate these two ratings for each threat in light of the recommended upgrades. Using an exterior explosive threat as an example, the installation of window retrofits (i.e., security window film, laminated glass, etc.) will not prevent the explosive attack from occurring, but it should reduce the impact of loss/injury caused by hazardous flying glass. Therefore, the impact of loss rating for an explosive threat would improve, but the vulnerability rating would stay the same.

Understanding threats

As responders we must understand threat components, which we must then counter. The threat has three components: aggressors; their tactics; and their associated weapons, explosives, and tools.

There are four types of aggressors that engineers must understand and plan against in a low-intensity conflict environment (Figure 3.3).

**Criminals** are subdivided into three categories: unsophisticated, sophisticated, and organized. Unsophisticated criminals are unskilled in the use of weapons and tools and have no formal organization. Their targets are those that meet their immediate needs, such as drugs, money, and pilferable items. They are interested in targets that pose little risk. Sophisticated criminals working singly are organized and efficient in the

---

**Figure 3.3** Threat assessment types.
use of certain weapons and tools. They target high-value assets and frequently steal large quantities. Organized criminal groups are sophisticated and rely on specialists to obtain equipment to achieve specific goals. Targets of organized criminal groups may include large quantities of money, equipment, arms, ammunition, and explosives.

*Protestors* may be categorized as vandals, activists, or extremists. Engineers must be concerned about all violent protestors. Protestors are politically or issue-orientated and act out of frustration, discontent, or anger. Their primary objectives include destruction and publicity.

Vandals and activists are unsophisticated and superficially destructive. They generally do not intend to injure people. Extremist groups are moderately sophisticated and more destructive. Their actions are frequently overt and may involve individuals as targets. Extremists, or terrorists are motivated by an ideology, a political cause, or an issue.

Terrorists commonly work in small, well-organized groups. They are sophisticated and possess efficient planning capabilities. Terrorist objectives include death, destruction, theft, and publicity. Terrorist groups are generally classified by their government affiliation.

*Subversives* are classified into two groups: saboteurs and spies. Saboteurs include guerrillas and commandos. They are very sophisticated and highly skilled and employ meticulous planning. Saboteurs commonly operate in small groups and have an unlimited arsenal. Their objectives include death and destruction. They often target mission-critical personnel, equipment, or operations. Spies are highly skilled and very sophisticated. They are generally foreign agents but frequently employ insiders. They target military information and attempt to avoid detection. In some cases, they may employ activists or other aggressors.

Individuals posing a threat employ a wide range of tactics to accomplish their objectives. These strategies have been categorized into 15 tactics, which are specific methods of achieving an aggressor’s goals. The following descriptions of aggressor tactics will assist engineer planners in developing protective methods, devices, facilities, and systems.

*Moving-vehicle bomb*: used when an aggressor’s goal is to damage or destroy a facility (or assets within a facility) or to kill people within the blast area. The moving-vehicle bomb is used in a suicide attack where an explosive-laden vehicle is driven into a facility and detonated.

*Stationary-vehicle bomb*: used when an aggressor’s primary objective is to damage or destroy a facility (or assets within a facility). This type of bomb maybe detonated by time delay or remote control. This attack has three versions:

1. An explosive-laden vehicle is driven to a preselected location and abandoned.
2. Explosives are placed in an unsuspecting person’s car. He then unknowingly delivers the bomb to the targeted facility.
3. Someone is coerced into delivering a vehicle bomb.

*Exterior attack*: used when an aggressor’s goal is to damage or destroy a facility (or assets within a facility) and kill or injure its occupants. This attack is conducted at close range to a facility or exposed asset. Using clubs, rocks, improvised incendiary devices, hand grenades, or hand-placed bombs, the aggressor attempts to inflict destruction and death.

*Standoff weapons attack*: used when an aggressor’s goal is to damage or destroy a facility (or assets within a facility) and kill or injure its occupants. These attacks are executed using military or improvised direct and indirect-fire weapons, such as antitank weapons and mortars.

*Ballistic attack*: used when an aggressor’s goal is to kill or injure a facility’s occupants. Using small arms at varying distances, the aggressor attempts to inflict death.

*Forced entry*: used when an aggressor’s goals are to steal or destroy assets, compromise information, or disrupt operations. Using small arms or forced-entry tools, the aggressor enters a facility through an existing passage or creates a new opening in the facility.

*Covert entry*: used when an aggressor’s goals are identical to those listed for the forced-entry tactic. The difference in these entries is that the aggressor will attempt to enter the facility covertly using false credentials. The aggressor may attempt to carry weapons or explosives into the facility.

*Insider compromise*: used when an aggressor’s goals are similar to those listed for the forced-entry tactic. The aggressor uses an insider (one who has legitimate access to a facility) to accomplish their prescribed objectives.

*Electronic eavesdropping*: used by an aggressor to monitor electronic emanations from computers, communications, and related equipment. This eavesdropping is normally done from outside a facility or restricted area.

*Acoustical eavesdropping*: an aggressor uses a listening device to monitor voice communication and other audible information.

*Visual surveillance*: used by aggressors employing ocular and photographic devices to monitor a facility, installation, or mission operations.

*Mail bombs*: used when the aggressor’s objective is to kill or injure people. Small bombs or incendiary devices are incorporated into envelopes or packages that are delivered to the targeted individual.

*Supplies bombs*: used when the aggressor’s objective is to kill or injure people or destroy facilities. Bombs or incendiary devices, generally larger than those found in mail bombs, are incorporated into various containers and delivered to facilities or installations.
Airborne contamination: used when the aggressor’s objective is to kill people. The aggressor uses chemical or biological agents to contaminate the air supply of a facility or installation.

Waterborne contamination: used when an aggressor’s objective is to kill people. The aggressor uses chemical, biological, or radiological agents to contaminate the water supply of a facility or installation.

Aggressors use various types of weapons, explosives, and tools to attain their objectives. Weapons range from clubs and rocks to mortars. Explosives are commonly used to destroy facilities and housing assets and to kill people.

Tools are primarily used in forced-entry operations to breach protective components or barriers. Understanding the aggressor’s options will aid the engineer in protecting forces from these items. Listed below are various weapons, explosives, and tools and their potential uses.

Rocks and clubs: used in exterior building attacks to damage exterior building components or exposed assets or to injure people.

Incendiary devices: used to damage the facility’s exterior or sabotage other assets. These include hand-held torches and improvised incendiary devices (IID). An example is a “Molotov cocktail.”

Firearms: used in a ballistic tactic to attack facility assets from a distance and in the forced-entry tactic to overpower guards. These include pistols, rifles, shotguns, and submachine guns, both military and civilian. Weapons capabilities are outlined in the Security Engineering Manual.

Antitank weapons and mortars: used in standoff attacks on facilities. For example, the direct-fire antitank weapons most often used by terrorists are the Soviet, rocket-propelled grenade RPG-7 and the U.S. light antitank weapon (LAW). These weapons increase the terrorist’s ability to penetrate and damage a facility and to kill or injure people. Mortars are indirect-fire weapons and include both military and improvised versions.

Nuclear, biological, and chemical: delivered as airborne or waterborne gases, liquids, aerosols, or solids. Very powerful chemical agents can be manufactured with relative ease from commercially available products. Biological agents can be grown in unsophisticated home laboratories. Radiological agents are radioactive elements that pose a potential threat to water supplies. They can be delivered in liquid or solid form.

Improvised explosive devices (IED): used in the exterior attack, mail and supplies bomb deliveries, forced-entry, covert-entry, and insider-compromise tactics to destroy assets and to injure or kill people. They are commonly “homemade” bombs made of plastic explosives or trinitrotoluene (TNT). Plastic explosives are chosen by terrorist and extremist protestor groups because they are easily molded, stable, and difficult to detect.

Hand grenades: used in exterior attacks to injure or kill people. These include common military antipersonnel and fragmentation hand grenades.
Vehicle bombs: used to destroy facilities and kill people. They contain large quantities of explosives and have the potential to do catastrophic damage.

Potential aggressors have access to a wide variety of tools, ranging from forced-entry tools, (hand and power tools, cutting torches, and burn bars) to sophisticated surveillance tools and devices. The quality and effectiveness of tools and devices used depends on the type of aggressor. The more sophisticated, trained, and organized the aggressor is, the more dangerous his tools and devices will be.

**Electronic risk assessment and vulnerabilities:**
**Computer/network internal and external threats**

The purpose of a threat risk assessment is to categorize enterprise assets, examine the different threats that may jeopardize them, and identify and correct the most immediate and obvious security concerns.

While taking tactical measures to correct immediate problems is important, understanding the different threats and risks will enable management to make informed decisions about security so they can apply appropriate, cost-effective safeguards in the longer term. This balanced approach allows for strategic positioning by logically applying risk-mitigation strategies in a controlled and economical manner rather than informal, and often expensive, implementations.

The threat, risk, and vulnerability assessment is an objective evaluation of threats, risks, and vulnerabilities in which assumptions and uncertainties are clearly considered and presented. Part of the difficulty of risk management is that both of the quantities with which risk assessment is concerned—potential loss and probability of occurrence—can be very difficult to measure. The chance of error in the measurement of these two concepts is large.

A risk with a large potential loss and a low probability of occurring is often treated differently from one with a low potential loss and a high likelihood of occurring. While in theory they may be of nearly equal priority, in practice it can be very difficult to prioritize both when faced with the scarcity of resources, especially time, in which to conduct the risk-management process.

One of the challenges in computer security is deciding how much security is necessary for proper control of system and network assets. This decision depends on conducting a threat assessment or, more specifically; what do you have and who would want it? While this is relatively simple to state, assessing a corporate network threat is not easy without a structured approach.

IT security risk/threat management assesses information security policies, processes, and technologies to identify weaknesses, categorize
security risks, and recommend improvements. Security assessment and risk analysis helps fortify the environment and improves compliance with industry regulations by providing a comprehensive assessment of each important aspect of the security program including:

- Internal and external controls
- Policies and procedures
- Gaps versus regulations and best practices
- Vulnerabilities and threats

**IT security risk assessment and analysis: Reporting objectives**

The report objectives of the security assessment and risk analysis are to provide management with clear and concise answers to the following questions:

- Within the scope of the control areas being tested, how well are information-based assets protected from internal and external threats?
- Are management, administrative, physical, and technical- and policy-based controls adequate?
- How do the controls compare to others in the industry?
- What is the quickest, most cost-effective way to manage risk to an acceptable level?

**Methodology**

Best-practice benchmarks may be used to identify select control gaps and strengths. A gap analysis-based approach allows a company sufficient control-visibility to set objectives and priorities for remediation efforts. It also allows documentation and representation of current control activities to regulatory auditors and examiners in the best context possible, as a best practice.

**The threat vulnerability assessment tool**

The threat vulnerability assessment requires organizations to conduct a risk vulnerability and threat assessment. The process concludes with a security overall assessment.

Sample risk assessment looking for the following issues and threats.

**Risk analysis description**

It is significant to note that a risk analysis, as defined by this methodology, is not an audit or an evaluation carried out by one entity upon another.
Chapter three: Threat/vulnerability assessments and risk analysis

It is, rather, a collaborative and objective fact-finding exercise between a managerial and technical team trained in this methodology and a managerial and technical team responsible for the information system(s) being analyzed. All findings included in the analysis must be substantiated by an objective reference (e.g., vulnerability scans, physical security reviews, incident reports, log records, etc.), which is then included in the appendices to the final risk analysis report. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

**Threat and vulnerability analysis**

The mission of the threat and vulnerability analysis team is to provide a detailed analysis, following the risk analysis methodology, of the specific threats and vulnerabilities associated with an IT system’s environment and configuration. The goal of this exercise is to develop an objective list of system vulnerabilities (flaws or weaknesses) that could be exploited by potential threat sources.

**Threat and vulnerability analysis description**

In addition to research and interviews, automated vulnerability scanning tools are used to identify system vulnerabilities efficiently. Frequently, vulnerabilities can be directly linked to missing or incomplete system-specific IT controls, or more broadly focused infrastructure-level common IT controls. The detailed analysis output from the “threat and vulnerability” step is the foundation upon which the next step in the risk analysis process is built.

**Attacks and threats**

- Handling destructive malware
- Understanding denial-of-service attacks
- Understanding hidden threats: corrupted software files
- Understanding hidden threats: rootkits and botnets
- Recognizing fake anti-viruses
- Avoiding the pitfalls of online trading
- Avoiding social engineering and phishing attacks
- Dealing with cyber bullies
- Identifying hoaxes and urban legends
- Preventing and responding to identity theft
- Recognizing and avoiding spyware
- Recovering from viruses, worms, and Trojan horses
- A working plan can be used to conduct the threat and vulnerability assessment as well as to define the components of the process including:
• Administrative safeguards
• Logical safeguards
• Physical safeguards
• Demographics of each physical location
• Access to each facility at each physical location
• Environmental factors associated with each physical location
• IT and business processes at each physical location
• A risk ranking matrix with a scoring mechanism that looks at vulnerability, as measured by probability of the threat occurring versus the impact of the loss and rules for scoring the risk
• A risk conveys the risk assessor’s judgment as to the nature and presence or absence of risks, along with information about how the risk was assessed, where assumptions and uncertainties still exist, and where policy choices will need to be made. Risk characterization takes place in both human-health and ecological risk assessments.
• Each component of the risk assessment (e.g., hazard assessment, dose-response assessment, exposure assessment) has an individual risk, assumptions, limitations, and uncertainties. The set of these individual risk characterizations provides the information basis to write an integrative risk-characterization analysis.
• The final, overall risk consists of the individual risk characterizations plus an integrative analysis. The overall risk characterization informs the risk manager and others about the approach to conducting the risk assessment.

**Principles of conducting risk characterizations**

A good risk characterization will restate the scope of the assessment, express results clearly, articulate major assumptions and uncertainties, identify reasonable alternative interpretations, and separate conclusions from policy judgments. Risk characterization policy calls for conducting risk characterizations in a manner that is consistent with the following principles.

• Transparency: The characterization should fully and explicitly disclose the risk assessment methods, default assumptions, logic, rationale, extrapolations, uncertainties, and overall strength of each step in the assessment.
• Clarity: The products from the risk assessment should be readily understood by readers inside and outside of the risk-assessment process. Documents should be concise, free of jargon, and should use understandable tables, graphs, and equations as needed.
• Consistent: The risk assessment should be conducted and presented in a manner which is consistent with Environmental Protection


Agency (EPA) policy, and consistent with other risk characterizations of similar scope prepared across programs within the EPA.

- Reasonable: The risk assessment should be based on sound judgment, with methods and assumptions consistent with the current state-of-the-science and conveyed in a manner that is complete, balanced, and informative.

In the field of risk assessment, characterizing the nature and magnitude of human-health or environmental risks is arguably the most important step in the analytical process. In this step, data on the dose-response relationship between an agent and outcomes are integrated with estimates of the degree of exposure of a population to characterize the likelihood and severity of risk. Although the purpose of risk characterizations is to make sense of the available data and describe what they mean to a broad audience, this step is often given insufficient attention in health risk evaluations. Too often, characterizations fail to interpret or summarize risk information in a meaningful way, or they present single numerical estimates of risk without an adequate discussion of the uncertainties inherent in key exposure parameters or the dose-response assessment, model assumptions, or analytical limitations. Consequently, many users of risk information have misinterpreted the findings of a risk assessment or have false impressions about the degree of accuracy (or the confidence of the scientist) in reported risk estimates.

In this article we collected and integrated the published literature on conducting and reporting risk characterizations to provide a broad, yet comprehensive, analysis of the risk characterization process as practiced in the United States and some other countries. Specifically, the following eight topics are addressed:

1. Objective of risk characterization
2. Guidance documents on risk characterization
3. Key components of risk characterizations
4. Toxicity criteria for evaluating health risks
5. Descriptors used to characterize health risks
6. Methods for quantifying human-health risks
7. Key uncertainties in risk characterizations
8. The risk decision-making process

The risk characterization guide is designed to provide risk assessors, risk managers, and other decision-makers an understanding of the goals and principles of risk characterization, the importance of planning and scoping for a risk assessment, the essential elements to address in a risk characterization, the factors that are considered in decision-making by
risk managers, and the forms that risk characterization takes for different audiences.

Conclusion

A risk conveys the risk assessor’s judgment as to the nature and presence or absence of risks, along with information about how the risk was assessed, where assumptions and uncertainties still exist, and where policy choices will need to be made. Risk characterization takes place in both human-health risk and ecological risk assessments.

Each component of the risk assessment (e.g., hazard assessment, dose-response assessment, exposure assessment) has an individual risk, assumptions, limitations, and uncertainties. The set of these individual risk characterizations provides the information basis to write an integrative risk-characterization analysis.

The final, overall risk consists of the individual risk characterizations plus an integrative analysis. The overall risk characterization informs the risk manager and others about the approach to conducting the risk assessment.