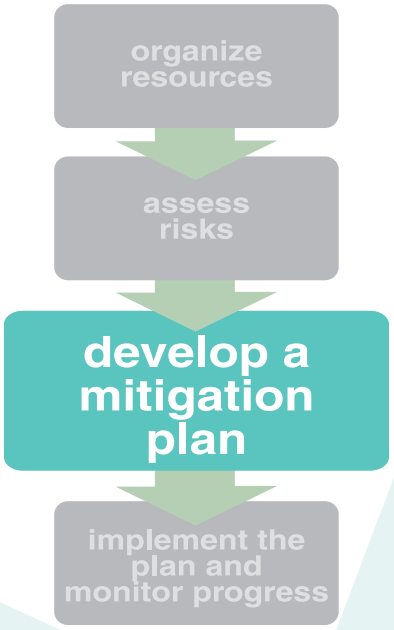
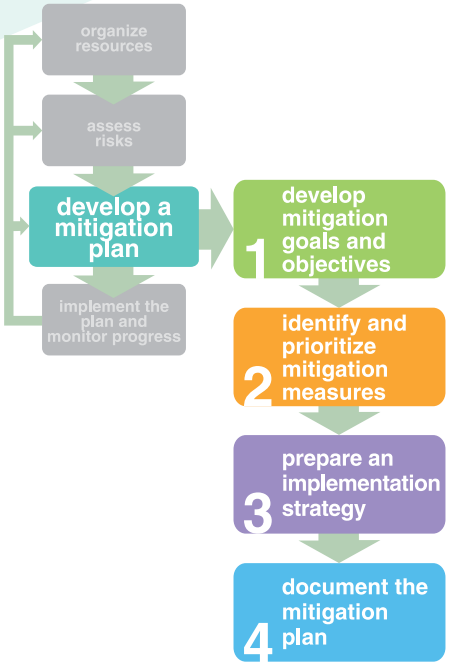
phase 3


organize resources
assess risks
develop a mitigation plan
implement the plan and monitor progress

3 develop a mitigation plan

Overview

The hazard identification and risk assessment described in Phase 2 will determine what facilities and systems in your jurisdiction are at highest risk. In Step 1 of Phase 3, you will develop goals and objectives for the protection of these assets to prevent or avoid an attack and to reduce losses in the event an attack occurs. Step 2 discusses the issues unique to identifying and prioritizing mitigation measures for terrorism and technological hazards. These measures primarily focus on creating a resilient, protective built environment. Step 3 highlights special considerations in developing an implementation strategy. Step 4 summarizes the important components to include in your terrorism and technological hazard mitigation plan. Cross-references are made to *Developing a Mitigation Plan: Identifying Mitigation Measures and Implementation Strategies* (FEMA 386-3).



Goals are general guidelines that identify what you want to achieve. They are usually long-term in nature.

Objectives define measurable strategies or implementation steps to attain a goal. They are shorter in range and more specific than goals.

Goals and objectives help determine where efforts and resources should be focused to maximize the effectiveness of mitigation-related activities. Whenever possible, mitigation goals and objectives should be multi-hazard in nature in order to provide the most comprehensive protection to your community or state. In addition to brainstorming, the planning team can identify additional goals and objectives in the following ways:

- **Review existing plans.** Review existing mitigation, comprehensive, and emergency plans, building upon and/or modifying existing initiatives to maximize coordination between plans and minimize conflicts and duplication of effort. To the extent possible, existing plans should be used to address the special problems posed by technological and other human-caused hazards rather than generating new, stand-alone documents.
- **Solicit public opinions.** Including the community in identifying goals and objectives will help ensure buy-in when mitigation measures are selected, and both the media and the Internet can be valuable communication tools. There are a number of methods for gauging public opinion:
  - Establish working groups or advisory committees
  - Hold town hall meetings
  - Administer surveys
  - Hold facilitated meetings with community representatives

While all of these methods can be effective on their own, it may be advantageous to combine multiple strategies, such as surveys and town hall meetings, in order to obtain the advantages of both a structured questionnaire as well as a free-flowing discussion.

Step 1
Develop Mitigation Goals and Objectives

The process for developing the mitigation goals and objectives that will shape your implementation strategy is the same whether you are addressing natural or human-caused hazards. As discussed in *Developing a Mitigation Plan: Identifying Mitigation Measures and Implementation Strategies* (FEMA 386-3), you will review the risk assessment and loss estimation findings to identify assets at greatest risk. Human-caused risk information should be combined with the findings for natural hazards to create a comprehensive picture of your community or state's vulnerabilities to both natural and human-caused hazards. Your terrorism and technological disaster mitigation goals, as with those for natural disasters, should strive to protect lives and property, reduce the costs of disaster response, and minimize disruption to the community or state following a disaster. See *Developing a Mitigation Plan* for more details on formulating and prioritizing your goals.

Sample Mitigation Goals and Objectives for Terrorism and Technological Hazard Mitigation

Goal 1: Reduce the community's risk of exposure to hazardous materials.

Objective 1: Install security measures at the anhydrous ammonia transfer and storage facility.

Objective 2: Increase the level of security of the facility using landscape design, lighting, and vehicle barriers.

Objective 3: Assess feasibility of hardening product storage and handling infrastructures.

Goal 2: Protect the community's water supply.

Objective 1: Install security measures at the city water treatment plant.

Objective 2: Secure all remote pump facilities.

Objective 3: Monitor for radiological, biological, and chemical contaminants.

Goal 3: Ensure that the city government has reliable communications systems.

Objective 1: Update the telecommunications capabilities of city government offices.

Objective 2: Create redundant/backup capability for landline telephone system.

Objective 3: Develop off-site backup of information technology systems.

Goal 4: Reduce risk to critical government facilities.

Objective 1: Increase vehicle standoff distance from the Emergency Operations Center.

Objective 2: Restrict parking and vehicle access to the underground parking garage at City Hall.

Step 2
Identify and Prioritize Mitigation Measures

Once you have developed goals and objectives for mitigation, you should identify specific measures to help you achieve them. As you consider mitigation options, keep in mind that attacks and accidents are functions of human activity, and the risk of such events is a characteristic of the target itself rather than of its geographic location. Clearly, there are areas in most communities where the chances of an attack or accident are considerably different from other parts of the jurisdiction—higher at industrial parks and critical facilities than in suburban residential neighborhoods, for example—but there is no such thing as a definable "terrorism zone" or "accident district" in the same sense as there are identifiable floodplains and seismic fault lines. Thus, it is not effective to protect people, buildings, and systems from human-caused hazards by simply relocating them as one could for some natural disasters.

Rather than removing potential victims from the hazard, then, mitigation strategies for human-caused hazards focus primarily on creating a built environment that is difficult to attack, resilient to the consequences of an attack or accident, and protective of its occupants should an incident occur. This can be accomplished through target hardening and other measures. Additional actions such as public awareness and education initiatives are not discussed in this guide but should be considered when formulating your mitigation strategy.

Target hardening measures range from small-scale projects, such as installing security fencing around an HVAC system's air intake, to community-wide initiatives, such as altering land use patterns to require buffer zones around campuses of high-risk buildings. Also, while some measures are highly specific in nature and function, others can meet multiple goals. For example, designing a building to resist the force of a bomb blast will also offer protection from windstorms, and requiring buffer zones around critical facilities can help meet open space requirements and protect wetlands. The planning team is encouraged to take advantage of these complementary approaches whenever possible.

Target hardening measures draw from a wide variety of disciplines, all of which, as discussed in Phase 1, should be represented on (or at least accessible to) the mitigation planning team. Potential hardening techniques and strategies are numer-

Taking Advantage of Existing Processes, Strategies, and Tools

Some measures and techniques used for mitigating natural hazards may also provide protection against human-caused hazards, such as:

Earthquake mitigation techniques that provide structural strengthening of buildings may help resist impact/explosion effects of bombs. Examples of such techniques include adding steel moment frames, shear walls, cross bracing, stronger floor systems, walls reinforced with shotcrete/fiber materials, columns reinforced with fiber wraps/steel jackets, tension/shear anchors, vibration dampers, and strengthening or providing additional detailing of the building's connections.

Fire mitigation techniques may help protect facilities against the effects of bombs and incendiary attacks. Examples of such techniques include improved sprinkler systems, increased use of fireproofing and/or fire-resistant materials, redundant water supplies for fire protection (day-to-day and alternative), and site setbacks.

High wind mitigation techniques that provide building envelope protection and structural strengthening may also help mitigate against impact/explosion effects of bombs. Examples of such techniques include openings using windows with impact-resistant laminated glazing, improving connections and the load path of the building, and adding/reinforcing shear walls.

Terrorism mitigation is becoming an integral part of multi-hazard mitigation, in process and often in practice. Additionally, a measure that addresses the fullest possible spectrum of natural and human-caused hazards will likely show the most cost-effectiveness.

The planning team should draw on all available sources of expertise when selecting specific measures, keeping in mind the overall objectives of maximizing opportunities for multi-hazard mitigation; promoting sustainability through choosing socially, economically, and environmentally beneficial solutions; supporting preparedness, response, and recovery; and ensuring cost-effectiveness.

ous, and a listing of every possible measure lies beyond the scope of this guidance. The list of potential measures provided below gives an overview of the techniques and strategies available. The Library in Appendix C contains references to many sources of information on these topics. The following section will discuss special considerations when evaluating measures to meet your goals and objectives.

Terrorism and Technological Hazard Mitigation Measures

The list of measures below is by no means exhaustive or definitive; rather, it is intended as a point of departure for identifying potential mitigation techniques and strategies in your community or state.

Site Planning and Landscape Design

- Implement Crime Prevention Through Environmental Design (CPTED)
- Minimize concealment opportunities in landscaping and street furniture, such as hedges, bus shelters, benches, and trash receptacles
- Design grounds and parking facilities for natural surveillance by concentrating pedestrian activity, limiting entrances/exits, and eliminating concealment opportunities
- Separate vehicle and pedestrian traffic
- Implement vehicle and pedestrian access control and inspection at perimeter (ensure ability to regulate flow of people and vehicles one at a time)
- Design site circulation to minimize vehicle speeds and eliminate direct approaches to structures
- Incorporate vehicle barriers such as walls, fences, trenches, ponds/basins, plantings, trees, sculptures, and fountains into site planning and design
- Ensure adequate site lighting
- Design signage for simplicity and clarity
- Locate critical offices away from uncontrolled public areas
- Separate delivery processing facilities from remaining buildings
- Maintain access for emergency responders, including large fire apparatus
- Identify and provide alternate water supplies for fire suppression
- Eliminate potential site access through utility tunnels, corridors, manholes, etc.

Architectural and Interior Space Planning

- Collocate/combine staff and visitor entrances; minimize queuing in unprotected areas
- Incorporate employee and visitor screening areas into planning and design
- Minimize device concealment opportunities such as mailboxes and trash receptacles outside screened areas
- Prohibit retail activities in non-secured areas
- Do not locate toilets and service spaces in non-secured areas
- Locate critical assets (people, activities, systems) away from entrances, vehicle circulation and parking, and loading and maintenance areas
- Separate high-risk and low-risk activities
- Separate high-risk activities from areas accessible to the public
- Separate visitor activities from daily activities
- Separate building utilities from service docks, and harden utilities
- Locate delivery and mail processing facilities remotely or at exterior of building; prevent vehicles from driving into or under building
- Establish areas of refuge; ensure that egress pathways are hardened and discharge into safe areas
- Locate emergency stairwells and systems away from high-risk areas
- Restrict roof access
- Ensure that walls, doors, windows, ceilings, and floors can resist forced entry
- Provide fire- and blast-resistant separation for sprinkler/standpipe interior controls (risers) and key fire alarm system components
- Use visually open (impact-resistant, laminated glass) stair towers and elevators in parking facilities
- Design finishes and signage for visual simplicity

Structural Engineering

- Create blast-resistant exterior envelope
- Ensure that structural elements can resist blast loads and progressive collapse
- Install blast-resistant exterior window systems (frames, security films, and blast curtains)
- Ensure that other openings (vents, etc.) are secure and blast-resistant
- Ensure that mailrooms are secure and blast-resistant
- Enclose critical building components within hardened walls, floors, and ceilings

(continued)

Mechanical Engineering

- Locate utility and ventilation systems away from entrances, vehicle circulation and parking, and loading and maintenance areas
- Protect utility lifelines (water, power, communications, etc.) by concealing, burying, or encasing
- Locate air intakes on roof or as high as possible; if not elevated, secure within CPTED-compliant fencing or enclosure
- Use motorized dampers to close air intakes when not operational
- Locate roof-mounted equipment away from building perimeter
- Ensure that stairways maintain positive pressure
- Provide redundant utility and ventilation systems
- Provide filtration of intake air
- Provide secure alternate drinking water supply

Electrical Engineering

- Locate utility systems and lifelines away from entrances, vehicle circulation and parking, and loading and maintenance areas
- Implement separate emergency and normal power systems; ensure that backup power systems are periodically tested under load
- Locate primary and backup fuel supplies away from entrances, vehicle circulation and parking, and loading and maintenance areas
- Secure primary and backup fuel supply areas
- Install exterior connection for emergency power
- Install adequate site lighting
- Maintain stairway and exit sign lighting
- Provide redundant telephone service
- Ensure that critical systems are not collocated in conduits, panels, or risers
- Use closed-circuit television (CCTV) security system

Fire Protection Engineering

- Ensure compliance with codes and standards, including installation of up-to-date fire alarm and suppression systems
- Locate fire protection water supply system critical components away from entrances, vehicle circulation and parking, and loading and maintenance areas
- Identify/establish secondary fire protection water supply
- Install redundant fire water pumps (e.g., one electric, one diesel); locate apart from each other
- Ensure adequate, redundant sprinkler and standpipe connections
- Install fire hydrant and water supply connections near sprinkler/standpipe connections
- Supervise or secure standpipes, water supply control valves, and other system components
- Implement fire detection and communication systems
- Implement redundant off-premises fire alarm reporting
- Locate critical documents and control systems in a secure yet accessible place
- Provide keybox near critical entrances for secure fire access
- Provide fire- and blast-resistant fire command center
- Locate hazardous materials storage, use, and handling away from other activities
- Implement smoke control systems
- Install fire dampers at fire barriers
- Maintain access to fire hydrants
- Maintain fire wall and fire door integrity
- Develop and maintain comprehensive pre-incident and recovery plans
- Implement guard and employee training
- Conduct regular evacuation and security drills
- Regularly evaluate fire protection equipment readiness/adequacy

Security

- Develop backup control center capabilities
- Secure electrical utility closets, mechanical rooms, and telephone closets
- Do not collocate security system wiring with electrical and other service systems
- Implement elevator recall capability and elevator emergency message capability
- Implement intrusion detection systems; provide 24-hour off-site monitoring
- Implement and monitor interior boundary penetration sensors
- Implement color closed-circuit television (CCTV) security system with recording capability
- Install call boxes and duress alarms
- Install public and employee screening systems (metal detectors, x-ray machines, or search stations)

Parking

- Minimize off-site parking on adjacent streets/lots and along perimeter
- Control all on-site parking with ID checks, security personnel, and access systems
- Separate employee and visitor parking
- Eliminate internal building parking
- Ensure natural surveillance by concentrating pedestrian activity, limiting entrances/exits, and eliminating concealment opportunities
- Use transparent/non-opaque walls whenever possible
- Prevent pedestrian access to parking areas other than via established entrances

While many benefits can be achieved through implementing mitigation measures, planners should be sensitive to potential negative impacts as well. For example, altering traffic patterns may increase commute times and distances, and reducing on-street parking may impact retail activity. Such considerations can be pivotal in determining the feasibility, viability, and potential for success of mitigation planning initiatives.

Prioritize Mitigation Measures

When prioritizing natural hazard mitigation measures, a benefit-cost analysis is generally conducted for each proposed measure. Several factors are considered, including:

- Cost(s) of the mitigation measure;
- Dollar value of risk reduction (i.e., loss of life, structure, content, and function) each time the hazard occurs (discussed in detail in *Understanding Your Risks: Identifying Hazards and Estimating Losses* [FEMA 386-2]);
- Frequency with which the benefits of the measure will be realized (i.e., frequency of hazard occurrence); and
- Time value of money (i.e., the fact that benefits and costs in the future are worth less than benefits and costs today).

These factors are then combined by calculating the net present value of aggregate future benefits and costs over the life span of the measure. For more details, see *Using Benefit-Cost Analysis in Mitigation Planning* (FEMA 386-5).

Three challenges arise when applying this benefit-cost framework to terrorism and technological disaster mitigation measures: (1) the probability of an attack or frequency of the hazard occurrence is not known; (2) the deterrence rate may not be known; and (3) the lifespan of the measure may be difficult to quantify.

First, the frequency factor is much more complex in the case of human-caused hazards than for natural hazards. While it is possible to estimate how often many natural disasters will occur (for example, a structure located in the 100-year floodplain is considered to have a 1 percent chance of being flooded in any given year), it is very difficult to quantify the likelihood of a terrorist attack or technological disaster. Quantitative methods to estimate these probabilities are being developed but have not yet been refined to the point where they can be used to determine incident probability on a facility-by-facility basis. Therefore, the planning team must use a qualitative approach based on threat and vulnerability considerations to estimate the relative likelihood of an attack or accident rather than the precise frequency. Such an approach is necessarily subjective but can be combined with quantitative estimates of cost-effectiveness (the cost of a measure compared to the value of the lives and property it saves in a worst-case scenario) to help illustrate the overall risk reduction achieved by a particular mitigation measure.

It is possible to determine fairly accurately how effective mitigation efforts will be in preventing damages from a given type of attack. The performance of many security and mitigation measures can be modeled using established engineering techniques. For example, structural engineers can determine how a hardening measure will protect a building's envelope. Naturally, the effectiveness of measures that rely on personnel or complex hardware can be more difficult to ascertain. For example, what is the probability that a security guard will fall asleep or that lightning will disable a perimeter sensor system?

Second, the deterrence or preventative value of a measure cannot be calculated if the number of incidents it averts is not known. Deterrence in the case of terrorism may also have a secondary impact in that once a potential target is hardened, a terrorist may turn to a less protected facility—changing the likelihood of an attack for both targets.

Third, the lifespan of a mitigation measure presents another problem when carrying out a benefit-cost analysis for terrorism and technological hazards. Future benefits are generally calculated for a natural hazard mitigation measure in part by estimating the number of times the measure will perform successfully over the course of its useful life. However, some protective measures may be damaged or destroyed in a single human-caused attack or accident. For example, blast-resistant window film may have performed to 100% effectiveness by preventing injuries from flying glass, but it may still need replacement after one "use." Other measures, such as a building setback, cannot be "destroyed" or "used up" per se. This is in contrast to many natural hazard mitigation measures, where the effectiveness and life span of a structural retrofit or land use policy are easily understood and their value over time quantifiable.

Step 3
Prepare an Implementation Strategy

As stated in the Foreword, this how-to guide assumes that your community or state is engaged in a natural hazards mitigation planning process and is intended to serve as a supplemental resource to help you address the unique risks associated with terrorism and technological hazards. If you have incorporated terrorism and technological hazards into a well-managed process, the implementation strategies and tools you use should enable you to effectively reduce your community or state's vulnerability to human-caused disasters as well. *Developing a Mitigation Plan* (FEMA 386-3) provides more details on preparing an implementation strategy.

Step 4
Document the Mitigation Plan

The mitigation plan for human-caused hazards will be based on the risk assessment conducted in Phase 2 and will include a comprehensive strategy to address the mitigation priorities developed in Phase 3, Step 2. This information, which should be integrated into the natural hazard mitigation plan, should include:

- A summary of the planning process, including the sequence of actions taken and a list of the team members and stakeholders who participated;
- The results of the risk assessment and loss estimation;
- Mitigation goals and objectives aimed at reducing or avoiding the effects of human-caused hazards;
- Mitigation measures that will help the community or state accomplish the established goals and objectives; and
- Implementation strategies that detail how the mitigation measures will be implemented and administered.

The hazard mitigation plan should serve as the focal point and basis for mitigation decisions for *all* hazards—natural and human-caused. As such, it should be written so that anyone who reads it can gain an understanding of current and future hazards and risks as well as the community's or state's intended solutions to those problems.

Ideally, terrorism and technological hazards will be incorporated into your existing mitigation plan; a single comprehensive plan is generally easier to manage and implement than a collection of stand-alone documents. However, some information may be of such high sensitivity that it should not be included in publicly available mitigation planning documents. Examples of such information include vulnerability studies of critical infrastructure and data on security plans and systems. This material should be treated as an addendum to the mitigation plan so that it is still part of the plan, but access to it can be controlled. For guidance on protecting sensitive information, see Phase 4, Consideration 1, Community Interest and Information Sensitivity.