ASSET VALUE, THREAT/HAZARD, VULNERABILITY, AND RISK 1

This chapter presents methodologies for architects, engineers, school administrators, and state and local officials working in the building sciences field to identify the most effective mitigation measures to achieve a desired level of protection against terrorist attacks. These methodologies will help designers define asset value and evaluate vulnerability assessment information for the purpose of integrating threat/hazard into a design basis. Architects and engineers will be able to identify the best and most cost-effective terrorism mitigation measures for each building's unique security needs. Mitigation measures are conceived by the design professional and are best incorporated into the building architecture, building systems, and operational parameters, with consideration for life-cycle costs. The methodologies described in this chapter can be used for new buildings during the design process, as well as for existing buildings undergoing renovation. A key tool in the assessment process is provided for the designer in the last section of this chapter, the Building Vulnerability Assessment Checklist.

In order to create a safe school environment, many factors must be considered. Figure 1-1 depicts the assessment process presented in this primer to help each school identify the best and most cost-effective terrorism mitigation measures for its own unique security needs. Section 1.1 identifies the value of a school's assets (e.g., people, buildings, equipment, and processes) that need to be protected, recognizing that students, faculty, and staff will always be a school's most vital asset requiring protection. Section 1.2 describes how to conduct a threat/hazard assessment to identify and define the threats and hazards that could cause harm to a school. Section 1.3 discusses how to perform a vulnerability assessment to identify school weaknesses that might be exploited by a terrorist or aggressor. Combining the results of the asset value, threat, and vulnerability assessments in Sections 1.1 through 1.3, the next step in the assessment process is to perform a risk assessment (Section 1.4) to determine to what degree a school's assets are vulnerable

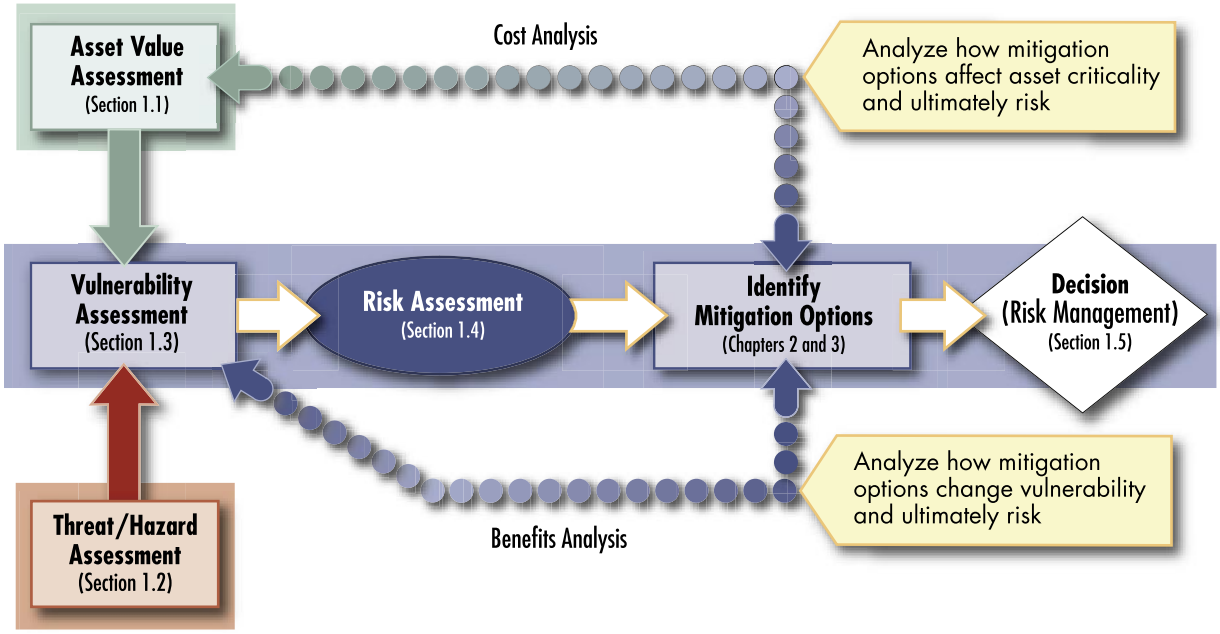

Figure 1-1 The assessment process model

to attack. The final step of the process is presented in Section 1.5, where risk management decisions are discussed to prioritize and decide on the best and most cost-effective terrorism mitigation measures to implement to achieve the desired level of protection.

A school assessment is best performed by engineering and security professionals who are experts in risk management, building design, blast effects, and chemical, biological, and radiological (CBR) attacks, as well as the latest antiterrorism (AT) security measures. If it is not feasible to hire professionals, members of the design community and/or school administrators can perform an assessment using the methodology presented in this primer. Some schools may choose to take a hybrid approach, hiring specialists or consultants to help perform individual portions of the assessment process.

1.1 ASSET VALUE ASSESSMENT

This section will describe how to perform an asset value assessment (the first step of the assessment process), to identify people

and the asset value. To facilitate identifying people and the value of a school's assets, it is useful to conduct interviews of the people who are most familiar with them. Inputs from school administrators, teachers, nurses, custodial staff, cafeteria staff, and students, as well as any others who can help identify the most valuable assets should be sought. In order to conduct productive interviews, a list of areas to be covered should be generated and prioritized prior to the actual interviews. Thorough planning and research to generate relevant questions will aid the process and yield better results.

An asset is a resource of value requiring protection.[1] An asset can be tangible (e.g., students, faculty, staff, school buildings, facilities, equipment, activities, operations, and information) or intangible (e.g., processes or a school's reputation). In order to achieve the greatest risk reduction at the least cost, identifying and prioritizing a school's critical assets is a vital first step in the process to identify the best mitigation measures to improve its level of protection prior to a terrorist attack. Recognizing that people are a school's most critical asset, the process described below will help identify and prioritize school infrastructure where people are most at risk and require protection.

Identifying a school's critical assets is accomplished in a two-step process:

Step 1: Define and understand the school's core functions and processes

Step 2: Identify school infrastructure

- Critical components/assets
- Critical information systems and data
- Life safety systems and safe haven areas
- Security systems

[1] Appendix B is a glossary of assessment and security terminology. Appendix C contains chemical and biological agent characteristics.

1.1.1 Identifying School Core Functions

The initial step of an asset value assessment is the determination of core functions and processes necessary for the school to continue to operate or provide services after an attack. The reason for identifying core functions/processes is to focus the design team and school administrators on what a school does, how it does it, and how various threats can affect the school. This provides more discussion and results in a better understanding of asset value. Factors that should be considered include:

- What are the school's primary services or outputs?
- What critical activities take place at the school?
- Who are the school's occupants or visitors?
- What inputs from external organizations are required for a school's success?

1.1.2 Identifying School Infrastructure

After the core functions and processes are identified, an evaluation of school infrastructure is the next step. To help identify and value rank infrastructure, the following should be considered, keeping in mind that the most vital asset for every school is its people:

- Identify how many people may be injured or killed during a terrorist attack that directly affects the infrastructure.
- Identify what happens to school functions, services, or student satisfaction if a specific asset is lost or degraded. (Can primary services continue?)
- Determine the impact on other organizational assets if the component is lost or can not function.
- Determine if critical or sensitive information is stored or handled at the school.
- Determine if backups exist for the school's assets.
- Determine the availability of replacements.

- Determine the potential for injuries or deaths from any catastrophic event at the school's assets.
- Identify any critical faculty, staff, or administration whose loss would degrade, or seriously complicate the safety of students, faculty, and staff during an emergency. [Consider first responders or the personnel responsible for shelter operations at a school that is a designated shelter for natural hazards.]
- Determine if the school's assets can be replaced and identify replacement costs if the school building is lost.
- Identify the locations of key equipment.
- Determine the locations of personnel work areas and systems within a school.
- Identify the locations of any personnel operating "outside" a school's controlled areas.
- Determine, in detail, the physical locations of critical support architectures:
  - Communications and information technology (IT - the flow of critical information)
  - Utilities (e.g., facility power, water, air conditioning, etc.)
  - Lines of communication that provide access to external resources and provide movement of students and faculty (e.g., road, rail, air transportation)
- Determine the location, availability, and readiness condition of emergency response assets, and the state of training of school staff in their use.

1.1.3 Quantifying Asset Value

After a list of a school's assets or resources of value requiring protection have been identified, they should be assigned a value. Asset value is the degree of debilitating impact that would be caused by the incapacity or destruction of the school's assets.

There are many scales that can be used, each with advantages and disadvantages. Because some people are used to working with linguistic scales, although many engineers and designers prefer numerical systems, this publication will use a combination of a seven-level linguistic scale and a ten-point numerical scale as shown in Table 1-1. Obviously, the key asset for every school is its people (e.g., students, faculty, and staff). They will always be assigned the highest asset value as in the example below.

Table 1-1: Asset Value Scale

Asset Value	
Very High	10
High	8-9
Medium High	7
Medium	5-6
Medium Low	4
Low	2-3
Very Low	1

Very High – Loss or damage of the school's assets would have exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services and core functions and processes.

High – Loss or damage of the school's assets would have grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core functions and processes for an extended period of time.

Medium High – Loss or damage of the school's assets would have serious consequences, such as serious injuries, or impairment of core functions and processes for an extended period of time.

Medium – Loss or damage of the school's assets would have moderate to serious consequences, such as injuries, or impairment of core functions and processes.

Medium Low – Loss or damage of the school's assets would have moderate consequences, such as minor injuries, or minor impairment of core functions and processes.

Low – Loss or damage of the school's assets would have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time.

Very Low – Loss or damage of the school's assets would have negligible consequences or impact.

Asset Value Example. A nominal list of assets for a typical high school with assigned value is presented in Table 1-2. Please note that this is a nominal example; each school should tailor its list to its own unique situation. In Section 1.4, the results of the asset value assessment will be combined with the results of a threat assessment (Section 1.2) and a vulnerability assessment (Section 1. 3) to determine total risk.

1.2 THREAT/HAZARD ASSESSMENT

After identifying asset value, the next step in the assessment process is to conduct a threat/hazard assessment wherein the threats or hazards are identified, defined, and quantified. Within the Department of Defense (DoD), intelligence community, and law enforcement, the term "threat" is typically used to describe the design criteria for terrorism or manmade disasters. Within the Federal Emergency Management Agency (FEMA) and other civil agencies, the term "hazard" is used in several different contexts. "Natural hazard" typically refers to a natural event such as an earthquake, a flood, or a wind disaster. "Manmade hazards" are "technological hazards" and "terrorism." These are distinct from natural hazards primarily in that they originate from human activity. Furthermore, "technological hazards" are generally assumed to be accidental, and their consequences are considered unintended. For the sake of simplicity, this primer will use the terms "threat" and "hazard" when referring to terrorism and manmade disasters, respectively.

Table 1-2: Nominal High School Asset Value Assessment

Asset	Value	Numeric Value
Students	Very High	10
Faculty	Very High	10
Staff	Very High	10
Designated Shelter (safe haven)	Very High	10
Main School Building	High	9
Teaching Functions	High	9
IT/Communications Systems	High	8
Utilities Associated with Shelter	Medium High	7
Utility Systems (gas, electrical, sewer/water)	Medium High	7
Nurses Station	Medium High	7
School/Student Records	Medium High	7
Transportation (buses and parking)	Medium High	7
Security Equipment (metal detectors, badge equipment)	Medium High	7
Administrative Functions	Medium	5
Temporary Classrooms (trailers)	Medium Low	4
Food Service (cafeteria/kitchen)	Medium Low	4
Library	Low	3
Custodial Functions	Low	3
Science Laboratories	Low	3
Vocational Equipment (shops)	Low	3
Indoor Sports Facilities	Low	2
Outdoor Sports Facilities	Very Low	1

For terrorism, the threat is from aggressors (those people with intent to do harm) that are known to exist, have the capability for hostile actions, and have expressed intentions for using hostile actions. They may seek publicity for their cause or political gain through their actions to injure or kill people, and destroy or damage facilities, property, equipment, or resources.

Aggressor tools can be forced entry tools, vehicles, or surveillance (visual/audio). Their weapons can be incendiary devices; small arms (rifles and handguns); stand-off military-style weapons (rocket propelled grenades or mortars); explosive devices; and CBR agents. Their tactics run the gamut: moving vehicle bombs; stationary vehicle bombs; exterior attacks (thrown objects like rocks, Molotov cocktails, hand grenades, or hand-placed bombs); stand-off weapons attacks (small arms, military or improvised direct and indirect fire weapons); covert entries (gaining entry by false credentials or circumventing security with or without weapons); mail bombs (delivered to individuals or institutions); airborne contamination (CBR agents used to contaminate the air, water, or food supply to a school); and waterborne contamination (CBR agents injected into the water supply of a school facility).

A threat assessment is a continual process of compiling and examining all available information concerning potential threats and manmade hazards. It can be broken down into two processes (1) defining threats and (2) identifying threat event profiles and tactics.

1.2.1 Threat Identification

The beginning point for security design is to define threats (hazards) and tactics that may be employed. From a physical attack viewpoint, schools maybe susceptible to attack by a number of different threats and tactics especially in areas of high risk. Schools are typically site constrained, have well defined traffic control and entry points, and operate on standard schedules. Designers and school administrators need to evaluate attack objectives, threat event profiles, and the effects or impact of the attack on the school and its occupants. It should also be noted that weapons and tactics change faster than the construction of schools. Table 1-3 provides a broad spectrum of manmade threats/hazards to consider and can be used as a tool in the threat assessment process. An extensive list of potential chemical and biological agents that can be used in terrorist attacks is provided in Appendix C. Blast range effects are indicated throughout Chapter 4.

Table 1-3: Event Profiles for Terrorism and Technological Hazards*

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Nuclear Device	Detonation of nuclear device underground, at the surface, in the air, or at high altitude.	Light/heat flash and blast/shock wave last for seconds; nuclear radiation and fallout hazards can persist for years. Electromagnetic pulse from a high-altitude detonation lasts for seconds and affects only unprotected electronic systems.	Initial light, heat, and blast effects of a subsurface, ground, or air burst are static and are determined by the device's characteristics and employment; fallout of radioactive contaminants may be dynamic, depending on meteorological conditions.	Harmful effects of radiation can be reduced by minimizing the time of exposure. Light, heat, and blast energy decrease logarithmically as a function of distance from seat of blast. Terrain, forestation, structures, etc., can provide shielding by absorbing and/or deflecting radiation and radioactive contaminants.
Biological Agent - Anthrax - Botulism - Bru cellosis - Plague - Smallpox - Tularemia - Viral Hemorrhagic Fevers - Toxins (Botulinum, Ricin, Staphylococcal Enterotoxin B, T-2 Mycotoxins)	Liquid or solid contaminants can be dispersed using sprayers/aerosol generators or by point or line sources such as munitions, covert deposits, and moving sprayers. May be directed at food or water supplies.	Biological agents may pose viable threats for hours to years, depending on the agent and the conditions in which it exists.	Depending on the agent used and the effectiveness with which it is deployed, contamination can be spread via wind and water. Infection can be spread via human or animal vectors.	Altitude of release above ground can affect dispersion; sunlight is destructive to many bacteria and viruses; light to moderate winds will disperse agents, but higher winds can break up aerosol clouds; the micro-meteorological effects of buildings and terrain can influence aerosolization and travel of agents.

Table 1-3: Event Profiles for Terrorism and Technological Hazards* (continued)

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Chemical Agent - Blister - Blood - Choking/Lung/ Pulmonary - Incapacitating - Nerve - Riot Control/Tear Gas - Vomiting	Liquid/aerosol contaminants can be dispersed using sprayers or other aerosol generators; liquids vaporizing from puddles/ containers; or munitions.	Chemical agents may pose viable threats for hours to weeks, depending on the agent and the conditions in which it exists.	Contamination can be carried out of the initial target area by persons, vehicles, water, and wind. Chemicals may be corrosive or otherwise damaging over time if not remediated.	Air temperature can affect evaporation of aerosols. Ground temperature affects evaporation of liquids. Humidity can enlarge aerosol particles, reducing the inhalation hazard. Precipitation can dilute and disperse agents, but can spread contamination. Wind can disperse vapors, but also cause target area to be dynamic. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place may protect students, faculty, staff, and property from harmful effects.
Radiological Agent - Alpha - Beta - Gamma	Radioactive contaminants can be dispersed using sprayers/aerosol generators, or by point or line sources such as munitions, covert deposits, and moving sprayers.	Contaminants may remain hazardous for seconds to years, depending on material used.	Initial effects will be localized to site of attack; depending on meteorological conditions, subsequent behavior of radioactive contaminants may be dynamic.	Duration of exposure, distance from source of radiation, and the amount of shielding between source and target determine exposure to radiation.
Improvised Explosive Device (Bomb) - Stationary Vehicle - Moving Vehicle - Mail - Supply - Thrown - Placed - Personnel	Detonation of explosive device on or near target; via person, vehicle, or projectile.	Instantaneous; additional secondary devices may be used, lengthening the time duration of the threat/hazard until the attack site is determined to be clear.	Extent of damage is determined by type and quantity of explosive. Effects generally static other than cascading consequences, incremental structural failure, etc.	Blast energy at a given stand-off is inversely proportional to the cube of the distance from the device; thus, each additional increment of stand-off provides progressively more protection. Exacerbating conditions include ease of access to target; lack of barriers/shielding; poor construction; and ease of concealment of device.

Table 1-3: Event Profiles for Terrorism and Technological Hazards* (continued)

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Arson/ Incendiary Attack	Initiation of fire or explosion on or near target via direct contact or remotely via projectile.	Generally minutes to hours.	Extent of damage is determined by type and quantity of device/accelerant and materials present at or near target. Effects generally static other than cascading consequences, incremental structural failure, etc.	Mitigation factors include built-in fire detection and protection systems and fire-resistive construction techniques. Inadequate security can allow easy access to target, easy concealment of an incendiary device, and undetected initiation of a fire. Non-compliance with fire and building codes as well as failure to maintain existing fire protection systems can substantially increase the effectiveness of a fire weapon.
Hazardous Material Release (fixed facility or transportation) - Toxic Industrial Chemicals and Materials (Organic vapors: cyclohexane; Acid gases: cyanogens, chlorine, hydrogen sulfide; Base gases: ammonia; Special cases: phosgene, formaldehyde)	Solid, liquid, and/or gaseous contaminants may be released from fixed or mobile containers.	Hours to days.	Chemicals may be corrosive or otherwise damaging over time. Explosion and/or fire may be subsequent. Contamination may be carried out of the incident area by persons, vehicles, water, and wind.	As with chemical weapons, weather conditions will directly affect how the hazard develops. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place can protect students, faculty, staff, and property from harmful effects. Non-compliance with fire and building codes as well as failure to maintain existing fire protection and containment features can substantially increase the damage from a hazardous materials release.
Armed Attack - Ballistics (small arms) - Stand-off Weapons (rocket propelled grenades, mortars)	Tactical assault or sniper attacks from a remote location.	Generally minutes to days	Varies, based upon the perpetrators' intent and capabilities.	Inadequate security can allow easy access to target, easy concealment of weapons, and undetected initiation of an attack.

Table 1-3: Event Profiles for Terrorism and Technological Hazards* (continued)

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Cyberterrorism	Electronic attack using one computer system against another.	Minutes to days.	Generally no direct effects on built environment.	Inadequate security can facilitate access to critical computer systems, allowing them to be used to conduct attacks.
Unauthorized Entry - Forced - Covert	Use of hand or power tools, weapons, or explosives to create a man-sized opening or operate an assembly (such as a locked door), or use false credentials to enter a building or simple covert entry.	Minutes to hours, depending upon the intent.	If goal is to steal or destroy physical assets or compromise information, the initial effects are quick, but damage may be long lasting. If intent is to disrupt operations or take hostages, the effects may last for a long time, especially if injury or death occurs.	Standard physical security building design should be the minimum mitigation measure. For more critical assets, additional measures, like closed circuit television (CCTV) or traffic flow that channels visitors past access control, aids in detection of this hazard.

*ADAPTED FROM: FEMA 386-7, *INTEGRATING HUMAN-CAUSED HAZARDS INTO MITIGATION PLANNING*, SEPTEMBER 2002.

1.2.2 Threat Definition

A threat (hazard) is any indication, circumstance, or event with the potential to cause loss of, or damage to an asset. It is important to understand who are the people with the intent to cause harm; or who, by process, materials, or proximity, can cause indirect harm to a school building. With the goal of reducing the potential risk of a school building, the design team and school administration should seek threat assessment information from local law enforcement, the local office of the Federal Bureau of Investigation (FBI), State Health Departments, the Department of Homeland Security (DHS), and the Homeland Security Offices (HSOs) at the state level. In many areas of the country, there are threat coordinating committees that facilitate the sharing of information. Local fire departments and hazardous materials (HazMat)

units will frequently understand the threat of technological hazards due to hazardous materials on school grounds as well as those in surrounding industries that could cause a collateral threat to schools. In many jurisdictions, the HazMat unit is part of the fire department.

After information on potential aggressors is gathered, it should be analyzed. A common method to evaluate terrorist threats uses five factors: existence, capability, history, intention, and targeting.

Existence addresses the questions: Who is hostile to our school building or community of concern? Are they present or thought to be present? Are they able to enter the country or are they readily identifiable in a local community upon arrival?

Capability addresses the questions: What weapons have been used in carrying out past attacks? Do the aggressors need to bring them into the area or are they available locally?

History addresses the questions: What has the potential threat element done in the past and how many times? When was the most recent incident and where, and against what target? What tactics did they use? Are they supported by another group or individuals? How did they acquire their demonstrated capability?

Intention addresses the questions: What does the potential threat element or aggressor hope to achieve? How do we know this (e.g., published in books or news accounts, speeches, letters to the editor, informant)?

Targeting addresses the questions: Do we know if an aggressor (we may not know which specific one) is performing surveillance on our school, nearby facilities, or facilities that have much in common with our school? Is this information current and credible, and indicative of preparations for terrorist operations (manmade hazards)?

The threat/hazard analysis for a school can range from a general threat/hazard scenario shared by all members of a community to a very detailed examination of specific groups, individuals, and tactics that must be repelled or defended against by means of school design. The Homeland Security Advisory System has five threat levels that provide a general indication of risk of terrorist attack. In Table 1-4, the five factors commonly used to evaluate terrorist threats have been layered onto the Homeland Security Advisory levels. It illustrates threat levels and provides a representation of the likelihood of a terrorist attack. If the anticipated threat or projected character/use of the facility warrant, a detailed threat analysis should be developed in coordination with local law enforcement, intelligence, and civil authorities in order to more quantitatively determine the vulnerability or risk. All schools should identify actions to be taken for each threat level. A table with specific recommendations for schools based on the Homeland Security Threat Advisory Level is presented in Chapter 3 (Table 3-3).

Table 1-4: Homeland Security Threat Conditions

Threat Level	Threat Analysis Factors				
	Existence	Capability	History	Intentions	Targeting
Severe (Red)	●	●	●	●	●
High (Orange)	●	●	●	●	❑
Elevated (Yellow)	●	●	●	❑	
Guarded (Blue)	●	●	❑		
Low (Green)	●	❑			

● Factor must be present ❑ Factor may or may not be present

Please note the DHS does not use these threat analysis factors to determine threat level.

SOURCE: COMMONWEALTH OF KENTUCKY OFFICE OF HOMELAND SECURITY.

1.2.3 Threat Assessment Products

A threat assessment is a continual process of compiling and examining all available information concerning potential threats and manmade hazards. The product of a threat assessment is a list

of threats and hazards with a threat rating assigned. The threat rating is a subjective judgment based on existence, capability, history, intention, and targeting. Often, information is sketchy and analysts must rely more on the judgment of experts, statistical probability, and occasionally assumptions to help quantify and qualify the threat (all assumptions should be documented). The same combination of linguistic scale and numerical scale used in the asset value assessment (Table 1-1) can be used for the threat assessment as presented in Table 1-5. Assessing terrorist threats is much more difficult than assessing the risk from natural hazards such as earthquakes, floods, and winds. Historical data form the basis of threat and locality indicates vulnerability to a great extent in regard to natural hazards. For terrorist threats, the likelihood of occurrence is less defined and the associated vulnerabilities have many considerations that impact making good risk management decisions.

Table 1-5: Threat Rating Scale

Threat Rating	
Very High	10
High	8-9
Medium High	7
Medium	5-6
Medium Low	4
Low	2-3
Very Low	1

Very High – Known aggressors or hazards, highly capable of causing loss of, or damage to the school exist. One or more vulnerabilities are present. The aggressors are known or highly suspected of having intent to exploit the school's assets and are known or highly suspected of performing surveillance on a facility.

High – Known aggressors or hazards, capable of causing loss of, or damage to the school exist. One or more vulnerabilities are present and the aggressors are known or reasonably suspected of having intent to exploit the school's assets.

Medium High – Known aggressors or hazards, capable of causing loss of, or damage to the school exist. One or more vulnerabilities are present and the aggressor is suspected of having intent to exploit the school's assets.

Medium – Known aggressors or hazards that may be capable of causing loss of, or damage to the school exist. One or more vulnerabilities may be present; however, the aggressors are not believed to have intent to exploit the school's assets.

Medium Low – Known aggressors or hazards that may be capable of causing loss of or damage to the school exist. Aggressors have no intent to exploit the school's assets.

Low – Few or no aggressors or hazards exist. Their capability of causing damage to the school's assets is doubtful.

Very Low – No aggressors or hazards exist.

Threat Assessment Example. A nominal list of threats/hazards with assigned threat rating is presented in Table 1-6. Please note that this is a nominal example; each school should tailor its list to its own unique situation.

Table 1-6: Nominal High School Threat Assessment

Threat/Hazard	Threat Rating	Numeric Threat Rating
Stationary vehicle bomb	Low	2
Attack with small arms	Medium Low	4
Hydrogen sulfide "stink bomb"	Medium	5
Forced entry at night to damage school property	Medium High	7
Electronic attack to destroy or alter school academic records	Medium High	7

1.2.4 Design Basis Threat

Traditionally, the building regulatory system has addressed natural disaster mitigation (hurricane, tornado, flood, earthquake, windstorm, and snow storm) through prescriptive building codes supported by well-established and accepted reference standards, regulations, inspection, and assessment techniques. Some manmade risks (e.g., HazMat storage) and specific societal goals (energy conservation and life safety) have also been similarly addressed. However, the building regulation system has not yet fully addressed most manmade hazards or terrorist threats.

Soon after September 11, 2001, the New York City Building Department initiated an effort to analyze the building code in relation to terrorist threats. The task force issued a report recommending code changes based on the attack on the World Trade Center. The National Fire Protection Association (NFPA) has a committee on premises security and security system installation standards. These advancements may some day result in the building regulatory system developing prescriptive building codes to mitigate security threats.

In the absence of such regulations, identifying design basis threats (e.g., threat tactics, weapons, tools, or explosives against which a building must be protected) should be considered as part of a school's threat assessment to facilitate the work of designers during new construction or rehabilitation of an existing school building. The DoD, General Services Administration (GSA), and Department of State (DOS) all have established processes to identify design basis threats for their facilities.

The typical building design and construction process is sequential, progressing from identifying building use and design goals through actual construction. This process is illustrated in Figure 1-2.

Figure 1-2 Typical building design and construction process

In every school design and renovation project, there are ultimately three choices of how to address the risk posed by terrorism:

1. Do nothing and accept the risk
2. Perform a risk assessment and manage the risk by installing reasonable mitigation measures to achieve a desired level of protection
3. Harden the building against all threats to achieve the least amount of risk

Figure 1-3 is a graphical representation of the three choices. Since September 11, 2001, terrorism has become a dominant concern. Life, safety, and security issues should be a design goal from the beginning for all schools.

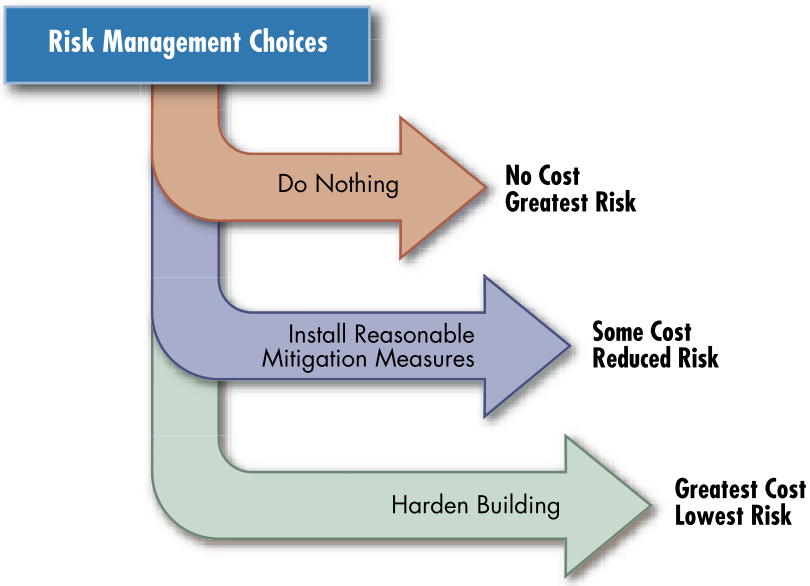

Figure 1-3 Risk management choices

1.3 VULNERABILITY ASSESSMENT

A vulnerability assessment evaluates vulnerability, or any weaknesses that can be exploited by an aggressor, of critical assets across a broad range of identified threats and provides a basis for determining mitigation measures for protection of people and critical assets.

The Building Vulnerability Assessment Checklist provided in Appendix F is based on the checklist developed by the Department of Veterans Affairs (VA) and compiles many best practices based upon technologies and scientific research to consider during the design of a new building or an assessment of an existing school building. It allows a consistent security evaluation of designs at various levels. The checklist can be used as a screening tool for an initial vulnerability assessment or be used by subject matter experts for a comprehensive vulnerability assessment of existing school buildings.

The assessment of any vulnerability of a school building should be done within the context of the defined threats and the value of the school's assets. That is, each element of the school building should be analyzed for vulnerabilities to each threat and a vulnerability rating should be assigned. The same combination of linguistic scale and numerical scale used in the asset value and threat assessments (Tables 1-1 and 1-5) can also be used for the vulnerability assessment as presented in Table 1-7. It should be noted that a vulnerability assessment may change the value rating of assets due to the identification of critical nodes or some other factor that makes the school's assets more valuable.

Table 1-7: Vulnerability Rating Scale

Vulnerability Rating	
Very High	10
High	8-9
Medium High	7
Medium	5-6
Medium Low	4
Low	2-3
Very Low	1

Very High – One or more major weaknesses have been identified that make the school's assets extremely susceptible to an aggressor or hazard.

High – One or more significant weaknesses have been identified that make the school's assets highly susceptible to an aggressor or hazard.

Medium High – An important weakness has been identified that makes the school's assets very susceptible to an aggressor or hazard.

Medium – A weakness has been identified that makes the school's assets fairly susceptible to an aggressor or hazard.

Medium Low – A weakness has been identified that makes the school's assets somewhat susceptible to an aggressor or hazard.

Low – A minor weakness has been identified that slightly increases the susceptibility of the school's assets to an aggressor or hazard.

Very Low – No weaknesses exist.

Vulnerability Assessment Example. To create the vulnerability assessment of a school, a site vulnerability assessment should be performed using the checklist in Appendix F. The results of the vulnerability assessment are then analyzed in conjunction with the results of the asset value and threat assessments developed earlier. Each asset/threat pair is then assigned a vulnerability rating as shown in Table 1-8 and forms the basis for identifying measures to mitigate threat vulnerability and improve protection of the building and its occupants. Please note that this is a nominal example; each school should tailor its list to its own unique situation.

Table 1-8: Nominal High School Vulnerability Assessment

	THREAT/HAZARD									
	Terrorist Act		Armed Attack		Unauthorized Entry		Low Level CBR Attack		Cyber-terrorism	
	Stationary Vehicle Bomb		Attack by Small Arms		Forced Entry at Night to Damage School Property		Hydrogen Sulfide "Stink Bomb"		Electronic Attack to Destroy or Alter School Academic Records	
ASSET	Vulnerability Rating		Vulnerability Rating		Vulnerability Rating		Vulnerability Rating		Vulnerability Rating	
Students	VH	10	H	9	VL	1	MH	7	VL	1
Faculty	VH	10	H	9	VL	1	MH	7	ML	4
Staff	VH	10	H	9	ML	4	MH	7	ML	4
Designated Shelter (safe haven)	H	9	L	3	ML	4	L	3	VL	1
Main School Building	VH	10	ML	4	M	5	L	3	VL	1
Teaching Functions	VH	10	VH	10	ML	4	H	9	L	3
IT/Communications Systems	VH	10	M	5	MH	7	L	2	MH	7
Utilities Associated with Shelter	H	8	ML	4	L	2	VL	1	VL	1
Utility Systems (gas, electrical, sewer/water)	MH	7	ML	4	M	5	L	2	VL	1
Nurses Station	H	9	H	8	M	6	L	3	VL	1
School/Student Records	H	9	L	3	M	6	L	2	MH	7
Transportation (buses and parking)	VH	10	H	9	M	6	L	3	VL	1
Security Equipment (metal detectors, badge equipment)	H	9	MH	7	M	6	L	2	VL	1
Administrative Functions	VH	10	H	8	M	6	MH	7	M	5
Temporary Classrooms (trailers)	VH	10	VH	10	MH	7	ML	4	VL	1
Food Service (cafeteria/kitchen)	VH	10	H	8	M	5	MH	7	VL	1
Library	VH	10	VH	10	MH	7	MH	7	ML	4
Custodial Functions	VH	10	ML	4	M	6	ML	4	VL	1
Science Laboratories	VH	10	M	5	H	8	L	3	VL	1
Vocational Equipment (shops)	VH	10	ML	4	H	8	L	3	VL	1
Indoor Sports Facilities	VH	10	ML	4	H	8	M	6	VL	1
Outdoor Sports Facilities	M	5	L	2	MH	7	L	2	VL	1

VH = Very High; H = High; MH = Medium High; M = Medium; ML = Medium Low; L = Low; VL = Very Low

1.4 RISK ASSESSMENT

Risk is the potential for a loss of or damage to an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it. Risk is based on the likelihood or probability of the hazard occurring and the consequences of the occurrence. A risk assessment analyzes the threat (probability of occurrence), and asset value and vulnerabilities (consequences of the occurrence) to ascertain the level of risk for each asset against each applicable threat/hazard. Thus, a very high likelihood of occurrence with very small consequences may require simple, low cost mitigation measures, but a very low likelihood of occurence with very grave consequences may require more costly and complex mitigation measures. The risk assessment provides engineers, architects, and school administrators with a relative risk profile that defines which assets are at the greatest risk against specific threats. Chapters 2 and 3 explore mitigation measures to reduce the vulnerability and risk for valuable assets with a high risk.

There are numerous methodologies and techniques for conducting a risk assessment. One approach is to assemble the results of the asset value assessment, threat assessment, and vulnerability assessment, and determine a numeric value of risk for each asset and threat/hazard pair in accordance with the following formula:

Risk = Asset Value x Threat Rating x Vulnerability Rating

The completed matrix provides a quantitative value for risk that can be converted into a linguistic value as shown in Table 1-9. The following rating system can be used for assessing the risk of schools.

Table 1-9: Risk Rating System

Risk	Risk Rating
≥ 261	Very High
201 - 260	High
141 - 200	Medium High
101 - 140	Medium
61 - 100	Medium Low
31 - 60	Low
1 - 30	Very Low

Very High – The potential for loss or damage of the school's assets is so great as to expect exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services, and core functions and processes.

High – The potential for loss or damage of the school's assets is so great as to expect grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core functions and processes for an extended period of time.

Medium High – The potential for loss or damage of the school's assets is such as to expect serious consequences (e.g., as serious injuries, or impairment of core functions and processes for an extended period of time).

Medium – The potential for loss or damage of the school's assets is such as to expect serious consequences (e.g., injuries, or impairment of core functions and processes).

Medium Low – The potential for loss or damage of the school's assets is such as to expect only moderate consequences (e.g., minor injuries, or minor impairment of core functions and processes).

Low – The potential for loss or damage of the school's assets is such as to expect only minor consequences or impact (e.g., a slight impact on core functions and processes for a short period of time).

Very Low – The potential for loss or damage of the school's assets is so low that there would only be negligible consequences or impact.

Because of the large amount of information in a risk assessment matrix, it is useful to assign a color code (red, yellow, or green) based on the total numeric value of risk determined based on the scale in Table 1-10.

Table 1-10: Risk Color Value System

	Low Risk	Medium Risk	High Risk
Risk Factors Total	1-60	61-175	≥ 176

As a minimum, mitigation measures to reduce risk and create an acceptable level of protection should be considered for those critical assets determined to be at highest risk.

Risk Assessment Example. A nominal risk assessment is presented in Table 1-11 based on the asset value, threat, and vulnerability assessment examples presented earlier. As mentioned previously, each school should tailor its list to its own unique situation.

Table 1-11: Nominal High School Risk Assessment Matrix

	Threat/Hazard				
	Terrorist Act	**Armed Attack**	**Unauthorized Entry**	**Low Level CBR Attack**	**Cyber-terrorism**
	Stationary Vehicle Bomb	Attack by Small Arms	Forced Entry at Night to Damage School Property	Hydrogen Sulfide "Stink Bomb"	Electronic Attack to Destroy or Alter School Academic Records
Students/Faculty/Staff	200	360	50	490	140
Asset Value Rating	10	10	10	10	10
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	9	1	7	2
Designated Shelter (safe haven)	180	120	200	210	70
Asset Value Rating	10	10	10	10	10
Threat Rating	2	4	5	7	7
Vulnerability Rating	9	3	4	3	1
Main School Building	180	144	225	189	63
Asset Value Rating	9	9	9	9	9
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	4	5	3	1
Teaching Functions	60	120	60	189	63
Asset Value Rating	3	3	3	3	3
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	10	4	9	3
IT/Communications Systems	160	160	280	112	392
Asset Value Rating	8	8	8	8	8
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	5	7	2	7
Utilities Associated with Shelter	112	112	70	49	49
Asset Value Rating	7	7	7	7	7
Threat Rating	2	4	5	7	7
Vulnerability Rating	8	4	2	1	1
Utility Systems (gas, electrical, sewer/water)	98	112	175	98	49
Asset Value Rating	7	7	7	7	7
Threat Rating	2	4	5	7	7
Vulnerability Rating	7	4	5	2	1
Nurses Station	126	224	210	147	49
Asset Value Rating	7	7	7	7	7
Threat Rating	2	4	5	7	7
Vulnerability Rating	9	8	6	3	1

Table 1-11: Nominal High School Risk Assessment Matrix (continued)

	Threat/Hazard				
	Terrorist Act	**Armed Attack**	**Unauthorized Entry**	**Low Level CBR Attack**	**Cyber-terrorism**
	Stationary Vehicle Bomb	Attack by Small Arms	Forced Entry at Night to Damage School Property	Hydrogen Sulfide "Stink Bomb"	Electronic Attack to Destroy or Alter School Academic Records
School/Student Records	126	84	210	98	343
Asset Value Rating	7	7	7	7	7
Threat Rating	2	4	5	7	7
Vulnerability Rating	9	3	6	2	7
Transportation (buses and parking)	140	252	210	147	49
Asset Value Rating	7	7	7	7	7
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	9	6	3	1
Security Equipment (metal detectors, badge equipment)	126	196	210	98	49
Asset Value Rating	7	7	7	7	7
Threat Rating	2	4	5	7	7
Vulnerability Rating	9	7	6	2	1
Administrative Functions	100	160	150	245	175
Asset Value Rating	5	5	5	5	5
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	8	6	7	5
Temporary Classrooms (trailers)	80	160	140	112	28
Asset Value Rating	4	4	4	4	4
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	10	7	4	1
Food Service (cafeteria/kitchen)	80	128	100	196	28
Asset Value Rating	4	4	4	4	4
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	8	5	7	1
Library	60	120	105	147	84
Asset Value Rating	3	3	3	3	3
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	10	7	7	4
Custodial Functions	60	48	90	84	21
Asset Value Rating	3	3	3	3	3
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	4	6	4	1

Table 1-11: Nominal High School Risk Assessment Matrix (continued)

	Threat/Hazard				
	Terrorist Act	**Armed Attack**	**Unauthorized Entry**	**Low Level CBR Attack**	**Cyber-terrorism**
	Stationary Vehicle Bomb	Attack by Small Arms	Forced Entry at Night to Damage School Property	Hydrogen Sulfide "Stink Bomb"	Electronic Attack to Destroy or Alter School Academic Records
Science Laboratories	60	60	120	63	21
Asset Value Rating	3	3	3	3	3
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	5	8	3	1
Vocational Equipment (shops)	60	48	120	63	21
Asset Value Rating	3	3	3	3	3
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	4	8	3	1
Indoor Sports Facilities	40	32	80	84	14
Asset Value Rating	2	2	2	2	2
Threat Rating	2	4	5	7	7
Vulnerability Rating	10	4	8	6	1
Outdoor Sports Facilities	10	8	35	14	7
Asset Value Rating	1	1	1	1	1
Threat Rating	2	4	5	7	7
Vulnerability Rating	5	2	7	2	1

1.5 THE RISK MANAGEMENT PROCESS

Risk management is the process of selecting and implementing mitigation measures to achieve an acceptable level of risk at an acceptable cost. Because it is cost-prohibitive to protect against the entire range of possible threats, it is important to develop a realistic prioritization of mitigation measures. When considering mitigation measures, the following factors should be considered:

- Results of the risk assessment, including asset value and asset vulnerabilities
- Costs of the mitigation measures

- The value of risk reduction to the school
- Frequency with which the benefits of the mitigation measures will be realized
- The deterrence or preventive value of the mitigation measures
- The expected lifespan of the mitigation measures and the time value of money

To evaluate prospective mitigation measures, the design team should first calculate new values of risk based on how the installation or use of mitigation measures would change vulnerability and/or asset values. Some mitigation measures will affect multiple asset/threat risk values. After the amount of risk reduction each mitigation measure will produce has been calculated, the cost of each mitigation measure should be estimated using resources such as R.S. Means Construction Cost Data. The final step is to perform a benefit/cost analysis to determine which mitigation measures will produce the greatest reduction of risk at an acceptable cost.

When dealing with manmade hazards and terrorism, it is much more difficult to predict how often an event will occur and the deterrent value of mitigation measures. Although there are historical data to help predict how often natural hazards such as floods or tornadoes occur in various regions, the probability or frequency of manmade hazards/threats is not known. Therefore, subjective approaches for frequency must be combined with quantitative estimates of cost-effectiveness.

Additionally, the deterrent or preventive value of a mitigation measure is also difficult to quantify. Deterrence, in the case of terrorism, may also have a secondary impact in that, once a school is "hardened," a terrorist may turn to a less protected building, changing the likelihood of an attack for both targets. For example, the Murrah Federal Building in Oklahoma City became the target of an aggressor when he was deterred from attacking his primary target, the FBI building, because it was too difficult to get the attack vehicle close to the target. He was able

to park immediately adjacent to the Murrah Federal Building and successfully target the Bureau of Alcohol, Tobacco, and Firearms (ATF).

All these factors should be considered when calculating the value of mitigation measures, and weighing their value against their cost. Ideally, sufficient resources would be available to achieve a desired level of protection against design basis threats through mitigation measures. This is not always the case, so it is also important that every school identify or designate an appropriate authority that is authorized to accept risk on behalf of the school. Sometimes when decisions are left up to committees or personnel at an inappropriate level, poor choices or decisions can be made.

It is also essential to maintain analytic integrity and objectivity during the assessment process in order to achieve an honest and unbiased risk assessment. Legitimate differences of professional opinion may occur; therefore, it is also important that the process be transparent and repeatable. For example, there could be an honest disagreement about the threat rating assigned to an "electronic attack to destroy school records." An open and repeatable methodology facilitates healthy debate to help the risk acceptance authority, who is ultimately responsible, make informed decisions.

In sum, the risk management process is a benefit/cost analysis to decide and prioritize which mitigation measures to implement to achieve the desired level of protection with available resources. This is accomplished by repeating risk assessment calculations adjusting for how mitigation measures change a school's asset values and vulnerabilities. As pointed out earlier, mitigation measures may also change how an aggressor views a school, thus changing the threat assessment as well.