STEP 3: VULNERABILITY ASSESSMENT

OVERVIEW

The third step in the assessment process is to prepare a vulnerability assessment of your assets that can be affected by a threat (see Figure 3-1). For this document, vulnerability is defined as any weakness that can be exploited by an aggressor to make an asset susceptible to hazard damage. A vulnerability assessment is an indepth analysis of the building functions, systems, and site characteristics to identify building weaknesses and lack of redundancy, and determine mitigations or corrective actions that can be designed or implemented to reduce the vulnerabilities. During this step, you will begin the analysis of your assets based on: a) the identified threat; b) the criticality of your assets: and c) the level of protection you may have chosen (i.e., your willingness or unwillingness to accept risk).

The vulnerability assessment process involves the following tasks:

- Organizing resources to prepare the assessment
- Evaluating the site and building
- Preparing a vulnerability portfolio
- Determining the vulnerability rating

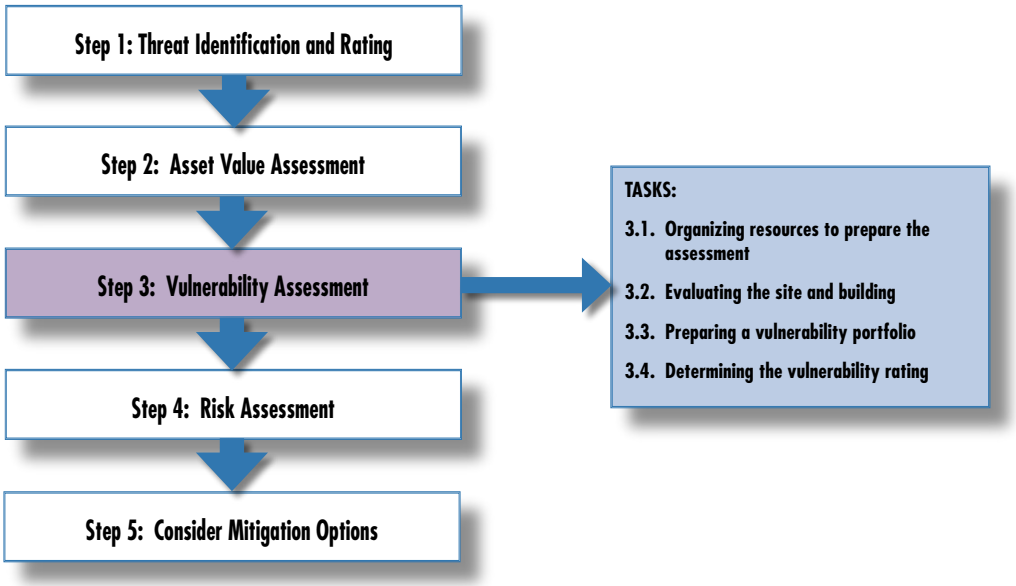

Figure 3-1 Steps and tasks

Organizing Resources to Prepare the Assessment (Task 3.1)

An important task during Step 3 is organizing your resources to prepare the assessment. This involves determining the level of the assessment you wish to perform and the skills of the team necessary to conduct the assessment.

Selecting the Assessment Team

The selection of the Assessment Team is probably the most critical task in the threat assessment process. An assessment has been found to be most effective when the Team is composed of senior individuals who have a breadth and depth of experience and understand other disciplines and system interdependencies. The Assessment Team leader will work with the building owner and stakeholders to:

- Determine the threat rating (Step 1)
- Determine the asset value and level of protection (Step 2)

The Assessment Team will coordinate the preparation of an assessment schedule, assessment agenda, and on-site visit assessments with the building stakeholders. It is important to emphasize that the Assessment Team should be composed of professionals capable of evaluating different parts of the buildings and familiar with engineering, architecture and site planning. Other members of the team may include law-enforcement agents, first responders, and building owners and managers.

Determining the Level of the Assessment

The level of the assessment for a given building is dependent upon a number of factors such as type of building, location, type of construction, number of occupants, economic life, and other owner specific concerns and available economic resources. The levels of the assessment provided in this How-To Guide are similar to the FEMA 310 process and provide increasing tiers of assessments. The underlying purpose is to provide a variable scale to meet benefit/cost considerations for a given building that meets the intent and requirements of available antiterrorism guidelines such as the DoD Minimum Antiterrorism Standards and the GSA Interagency Security Criteria.

Tier 1. A Tier 1 assessment is a screening phase that identifies the primary vulnerabilities and mitigation options, and is a "70 percent" assessment (see Table 3-1). A Tier 1 assessment can typically be conducted by one or two ex-

perienced assessment professionals in approximately 2 days with the building owner and key staff; it involves a "quick look" at the site perimeter, building, core functions, infrastructure, drawings, and plans. A Tier 1 assessment will likely be sufficient for the majority of commercial buildings and other non-critical facilities and infrastructure.

Tier 2. A Tier 2 assessment is a full on-site evaluation by assessment specialists that provides a robust evaluation of system interdependencies, vulnerabilities, and mitigation options; it is a "90 percent" assessment solution (see Table 3-2). A Tier 2 assessment typically requires three to five assessment specialists, can be completed in 3 to 5 days, and requires significant key building staff participation (e.g., providing access to all site and building areas, systems, and infrastructure) and an indepth review of building design documents, drawings, and plans. A Tier 2 assessment is likely to be sufficient for most high-risk buildings such as iconic commercial buildings, government facilities, schools, hospitals, and other designated high value infrastructure assets.

Tier 3. A Tier 3 assessment is a detailed evaluation of the building using blast and weapons of mass destruction (WMD) models to determine building response, survivability, and recovery, and the development of mitigation options. A Tier 3 assessment (see Table 3-3) typically involves engineering and scientific experts and requires detailed design information, including drawings and other building information. Modeling and analysis can often take several days or weeks and is typically performed for high value and critical infrastructure assets. The Assessment Team is not defined for this tier; however, it could be composed of 8 to 12 people.

Table 3-1: Tier 1 - Screening Phase

Task	Building Type	Team Composition	Duration	Activity
Information Gathering and Review	Standard commercial office building	1 Site and Architectural 1 Security Systems and Operations	1 day	Review technical area and general site analysis
On-site Evaluation			1 day per assessor	• Complete the Critical Function and Critical Infrastructure matrices; perform a limited technical review using the Building Vulnerability Assessment Checklist; input site, vulnerability, and mitigation information into the database; write reports • Prepare a verbal or PowerPoint presentation with key findings to review with building owners' and stakeholders' major findings • Receive input on the assessment process
Develop Mitigation Options			Typically 1 to 3 days per assessor	• Prepare a Preliminary Report, including findings and feedback from stakeholders. This report should include concept and cost mitigation options. • Prepare a written Final Report that lists the vulnerabilities, observations, and mitigation options. Very rough order of magnitude cost estimates may be developed using standard unit costs for blast, CBR, and physical security infrastructure and equipment. • Prepare a Vulnerability Portfolio with recommendations for incorporation into Emergency Operations, Disaster Recovery, and other plans or procedures

Table 3-2: Tier 2 - Full On-site Evaluation

Task	Building Type	Team Composition	Duration	Activity
Information Gathering and Review	High-risk or iconic buildings Commercial buildings, government facilities, schools, and hospitals Designated high asset value infrastructure	1 Site and Architectural (recommended as Team leader) 1 Structural and Building Envelope 1 Mechanical, Electrical, and Power Systems and Site Utilities 1 Landscape Architect 1 IT and Telecommunications 1 Security Systems and Operations	1 day per assessor	Review technical area and general site analysis collected during the Tier 1 assessment
On-Site Evaluation			2 to 4 days per assessor	• Complete the Critical Function and Critical Infrastructure matrices; perform a limited technical review using the Building Vulnerability Assessment Checklist; input site, vulnerability, and mitigation information into the database; write reports • Prepare a verbal or PowerPoint presentation with key findings to review with building owners' and stakeholders' major findings • Receive input on the assessment process
Develop Mitigation Options			1 to 3 days per assessor	• Prepare a Preliminary Report, including findings and feedback from stakeholders. This report should include concept and cost mitigation options. • Prepare a written Final Report that lists the vulnerabilities, observations, and mitigation options. Very rough order of magnitude cost estimates may be developed using standard unit costs for blast, CBR, and physical security infrastructure and equipment. • Prepare a Vulnerability Portfolio with recommendations for incorporation into Emergency Operations, Disaster Recovery, and other plans or procedures

Table 3-3: Tier 3 - Detailed Evaluation

Building Type	Team Composition	Activity
High value and critical infrastructure assets	1 Site and Architectural - Team leader 1 Structural and Building Envelope 1 Mechanical, Electrical, and Power Systems and Site Utilities 1 IT and Telecommunications Modeler 1 Security Systems and Operations 1 Explosive Blast Modeler 1 CBR Modeler 1 Cost Engineer 1 Landscape Architect	• A typical Tier 3 Assessment Team will use the results of the Tier 2 assessment and involve modeling and analysis of the building and related systems using advanced blast and WMD models and applications. Blast analysis will include structural progressive collapse, glazing, and effects of building hardening. CBR analysis should evaluate the effects of the agents released externally and internally to provide the dispersion, duration, and exposure of the building systems and occupants. The IT and Telecommunications Modeler should evaluate effects on all IT systems assuming cascading equipment failure and long-term access denial to critical equipment, data, and on-site administrative capability. • The Tier 3 assessment will provide detailed building response, survivability, and recovery information used to develop enhanced and accurate costing of mitigation options.

Evaluating the Site and Building (Task 3.2)

Understanding the type, nature, and geographic range of threats (Step 1) that can occur at your site or building, as well as the associated exposure of your assets (Step 2) is essential to conducting a vulnerability analysis. Each building, even if on the same campus or the same general area, can have different priority threats and hazards. A well-prepared risk manager must be aware of the types of threat and hazard events that can occur, the areas and resources most at risk, and the potential costs and losses that could accompany a threat or hazard event.

To prepare an effective assessment, the following activities should take place:

1. **Pre-Meeting and Preparation of a Schedule and Tentative Agenda.** Before conducting the on-site building evaluation, a coordination meeting should take place. During this meeting, the type of assessment to be conducted, personnel availability, schedules, and outputs should be discussed in detail. In addition, firm timetables and an agenda for on-site visits should be discussed. The agenda schedule should include the sites to be evaluated and special areas to be protected. Worksheets 3-1 and 3-2 have been developed to aid in this process.

2. **On-Site Meeting(s).** For each assessment, a preparation meeting will take place with key stakeholders. Upon arrival at the site or building, the Team should have an introduction meeting with key staff, review the available information, and review the vulnerability portfolio (Task 3.3). As a minimum, recommended building personnel attendees should include:

    - Site or building owner
    - Chief of engineering
    - Chief of security
    - Chief of IT
    - Emergency manager

Other attendees may include:

- Union or employee representatives
- Local law enforcement, fire, and EMS representatives
- State or county representatives

- Local utility, telecommunications, and services (waste, security services, etc.)
- Administration, food services, laboratory, and other critical function representatives

For the assessment to be successful, building stakeholders should participate as key members, providing on-site access to all buildings and areas. In addition, they should participate in interviews, and provide comments on current strengths and weakness of plans and procedures, including facility access, personnel movement, operations and maintenance, and security alerts.

3. **Windshield Tour(s).** After the introduction meeting, the Assessment Team and stakeholders should conduct a "windshield" tour or walk-around of the key facilities. The Assessment Team may find areas that require special attention and feel the need to make adjustments to the assessment agenda (Worksheet 3-2).

4. **Assessment Background Information.** After the on-site tour, the Assessment Team and stakeholders are ready to conduct the on-site assessment. Completing the matrices provided in this How-To Guide for conducting the threat assessment will take approximately 4 to 8 hours, using an interview and consensus approach around a table. During these discussions, the Team should prepare worksheets provided in Steps 1 and 2. They will determine:
   - Threats that are a priority concern for your site, building, and related infrastructure (Worksheets 1-1 and 1-2)
   - The assets of your area, building or site that can be affected by a threat (Worksheet 2-1)

5. **Review Key Documents.** The Assessment Team will review or evaluate a number of plans, procedures, and policies. The list below provides some of the documents that need to be reviewed by the Team before conducting the assessment. How to gather this information is described in Steps 1 and 2.
   - Prior vulnerability assessment data
   - Emergency response and disaster recovery plans
   - Security master plan (including detection/delay/assess)

- Security inspection results
- HazMat plans
- Policy and legal requirements
- Federal, State, and local law enforcement threat assessments
- Site plans of utility and communications systems
- Floor plans for all facilities identified as important (including those listed above)
- Floor plans and locations of modified and abandoned facilities
- Structural drawings of key facilities
- New project drawings for fences, security, and buildings
- Security system drawings
- Historical reports
- Local zoning ordinances
- Comprehensive plans
- Development plans
- Information on the facility systems operations capability
- Information on agreements with the surrounding community and Federal agencies
- Information on incidents within the building (i.e., misconduct information)
- Population statistics
- Manpower surveys
- Other documents determined by the Team to be important

6. **Review Emergency Procedures.** The Assessment Team and building stakeholders should review the security master plan, and the engineering operations and maintenance, emergency operations, and disaster recovery plans to understand the critical assets of the building and establish a baseline organization response and recovery capability in case of an attack or event. The impact of many vulnerabilities can be reduced or eliminated by simple changes in plans, policies, and procedures. As part of the screening phase review, the following areas should be considered:

- Emergency notification procedures
- Emergency evacuation procedures
- First responder access and routing
- Shelter-in-place procedures
- Designated shelter capacities and travel routes
- Off-site rally point and roll call
- Emergency engineering systems shutdown (HVAC, electrical, information technology (IT)/telecommunications)
- Portable protective equipment (indoor air filters, sampling kits, first aid)
- Personal protective equipment (PPE)
- Exercise of plans

7. **Prepare the Assessment.** Preparing the assessment can be as simple as a quick review and analysis of existing documents and a short walk around the site, or a more detailed in-depth review and analysis of the documents, plans, and other information and a thorough walk-through of the building, including utility spaces, basements, crawl spaces, attics, and vault (see Tables 3-1, 3-2, and 3-3). The following are recommended when conducting the different types of assessments.

   For Tier 1 Screening Evaluation, the analysis should include, at a minimum:

   - Perimeter identification
   - Vehicle and pedestrian entry access control points
   - Security operations function
   - EOC (or function)
   - Primary point of entry of utilities and telecommunications
   - Critical functions
   - Critical infrastructure
   - Key staff
   - Off-site rally point and other Emergency Management procedures (PPE, mass notification, etc.)

For Tier 2 On-Site Evaluation, the analysis should include, at a minimum:

- Tier 1 information
- Detailed inspection and route tracing of primary utilities and telecommunications
- Detailed review of HVAC system and operating parameters
- Detailed review of electric power and generator capacity (life safety, data centers, communications, etc.)
- Detailed review of structural and envelope system (column-beam connections, materials, clips, glazing)
- Detailed review of Security Master Plan, Emergency Management Plan, other related plans and Memorandums of Understanding (MOU) (Continuity of Operations [COOP], Continuity of Government [COG], Certified Emergency Management Plan [CEMP], etc.)

For Tier 3, Detailed Evaluation, the analysis should include, at a minimum:

- Tier 2 information
- Systems interdependencies on-site and off-site (utility vaults, communications central office trunks, transportation nodes, logistics, etc.)
- Advanced blast and CBR modeling of building and systems (structural damage, interior and exterior plume dispersion, safe haven areas)
- Advanced evacuation planning and routing to include test of mass notification system, training, and exercises
- Advanced disaster response and recovery planning in conjunction with neighbors and local government

8. **Data Gap Analysis.** The Assessment Team may feel that the data gathered for on-site assessment are not enough. The Team should assess the following information:
   - Do we know where the greatest damages may occur in the threat/hazard areas?
   - Do we know whether critical facilities will be operational after a threat/hazard event?

- Are there enough data to determine which assets are subject to the greatest potential damages?
- Are there enough data to determine whether significant elements of the community are vulnerable to potential threats?
- Are there enough data to determine whether certain areas of historic, environmental, political, or cultural significance are vulnerable to potential threats?
- Is there concern about a particular threat because of its severity, frequency, or likelihood of occurrence?
- Are additional data needed to justify the expenditure of community or state funds for mitigation initiatives?

If the Team decides that more data will be beneficial to conduct the assessment, a determination should be made as to what type of data are needed and what resources are available for collecting new data. If stakeholders and the Team agree on collecting new data, the Team needs to prioritize areas for additional data collection.

Preparing a Vulnerability Portfolio (Task 3.3)

To carry out the assessment, the Team should have a vulnerability portfolio available. This portfolio should include the following:

- ❍ Assessment agenda (Worksheet 3-2)
- ❍ Assessment background information (to be collected by Assessment Team and building owners)
- ❍ Threats rating (Worksheets 1-1 and 1-2)
- ❍ Asset value ranking worksheet (Worksheet 2-1)
- ❍ Key documents (plans, procedures, and policies, see Task 3.2)
- ❍ Emergency procedures (baseline organization response and recovery capability in case of an attack or event, see Task 3.2)
- ❍ Building Vulnerability Assessment Checklist (Appendix A)
- ❍ Risk assessment matrices (Worksheets 4-1 and 4-2, described in Step 4)

- Prioritization of observations in the checklist (Worksheet 4-3)

- Risk Assessment Database (if assessment is going to be automated – see Appendix B)

The Building Vulnerability Assessment Checklist, the Pre-Assessment Screening Matrix, and the Risk Assessment Database are explained below.

Building Vulnerability Assessment Checklist. Appendix A includes the Building Vulnerability Assessment Checklist, which compiles many best practices based on technologies and scientific research to consider during the design of a new building or renovation of an existing building. It allows a consistent security evaluation of designs at various levels.

The Checklist is a key tool in the preparation of the threat assessment and a fundamental element of your vulnerability portfolio. When performing a walk-through of the facility to be assessed, the Team should use the Checklist as a screening tool for preparing the vulnerability assessment and make observations when reviewing the questions included in the Checklist.

The Checklist is organized into 13 sections. To conduct a vulnerability assessment of a building or preliminary design, each section of the Checklist should be assigned to an engineer, architect, or subject matter expert who is knowledgeable and qualified to perform an assessment of the assigned area. Each assessor should consider the questions and guidance provided to help identify vulnerabilities and document results in the observations column. The observations made during this Step will be prioritized during Step 4. The observations in the Checklist should be supplemented with photographs, if possible.

Risk Assessment Database. To support the building assessment process, a simple and easy to use Risk Assessment Database application is provided with this manual (see Appendix B). This database was originally developed for the Department of Veterans Affairs (VA) through the National Institute of Building Sciences (NIBS). It has already been used in the assessment of over 100 hospitals, office buildings, data centers, and other facilities across the United States. FEMA modified this database in order to make it easy-to-use for commercial buildings. The database is a stand-alone application that has functions, folders to import and display digital photos, emergency plans, digital floor plans, and certain HAZUS-MH products. Information retrieved from HAZUS-MH and existing commercial off the shelf (COTS) software such as Facility Condition Assessment, Work Order, Real Estate, and Space and

Planning applications can be used in conjunction with the database for the assessment. Site, Team, and other general information is collected and inputted using screens. This database contains the basic information included in the Building Vulnerability Assessment Checklist. The Risk Assessment Database is an integral part of this How-To Guide.

Using the Building Vulnerability Assessment Checklist and the Risk Assessment Database. For all types of evaluations (Tiers 1, 2, and 3) the Building Vulnerability Assessment Checklist and the Risk Assessment Database can be used to collect and report information related to the building infrastructure. In practice, many assessment Team members will find it easier to use a paper copy of the checklist while walking the site and enter their field observations when back in the office. The newer tablet personal computers (PCs) can be used for direct data entry. Typically, each assessment Team member will be responsible for completing several sections of the checklist; the amount and detail of information that can be acquired and inputted into the checklist will depend upon the on-site time available and the amount of information that is readily available versus difficult to find. For example, ideally, a full set of computer-aided design (CAD) drawings would be used to evaluate the site, architectural elements, structural features, mechanical and electrical systems, and security systems. However, if CAD drawings are not available, often the Disaster Management Office, Safety Officer, or building engineer will have 8½ x 11 inch site and floor plans that can be used in hard copy, scanned, and then color coded using simple photoshop applications. If no plans are available, a picture of the fire evacuation plan on each floor should be taken.

At the end of the day, after each assessment Team member has inputted his or her observations into the database, the Team should meet to review the observations and develop the vulnerability and mitigations list. The vulnerabilities can be grouped by campus, site, or individual building and each vulnerability can be given a priority; a vulnerability can have multiple mitigation options and each option should have a Rough Order of Magnitude Cost.

By reviewing the Critical Functions and Critical Infrastructure matrices and the color coded site and floor plans, the assessment Team can identify those functions and infrastructure that are collocated or are a single-point vulnerability (see Task 3.4) where multiple assets are susceptible to an event. A key risk reduction strategy is to build redundancy into the system by providing alternate means of service and places to connect temporary supplies for utilities and telecommunications, disperse or have alternate sites for key staff and functions, and have multiple means of communication for shelter-in-place and evacuation decisions.

Determining the Vulnerability Rating (Task 3.4)

This task involves determining a vulnerability rating that reflects the weakness of functions, systems, and sites in regard to a particular threat. Weakness includes the lack of redundancies that will make the building system operational after an attack.

Redundancy Factor

A terrorist selects the weapon and tactic that will cause harm to people, destroy the infrastructure, or functionally defeat the target. The function and infrastructure vulnerability analysis will identify the geographic distribution within the building and interdependencies between critical assets. Ideally, the functions should have geographic dispersion as well as a recovery site or alternate work location. However, some critical functions and infrastructure do not have a backup, or will be determined to be collocated and create what are called single-point vulnerabilities. Identification and protection of these single-point vulnerabilities is a key aspect of the assessment process. Concerns related to common system vulnerabilities are:

- No redundancy
- Redundant systems feed into single critical node
- Critical components of redundant systems collocated
- Inadequate capacity or endurance in post-attack environment

Identification and protection of these single-point vulnerabilities will help you to determine a more accurate vulnerability rating for your assessment. Figure 3-2 shows common system vulnerabilities.

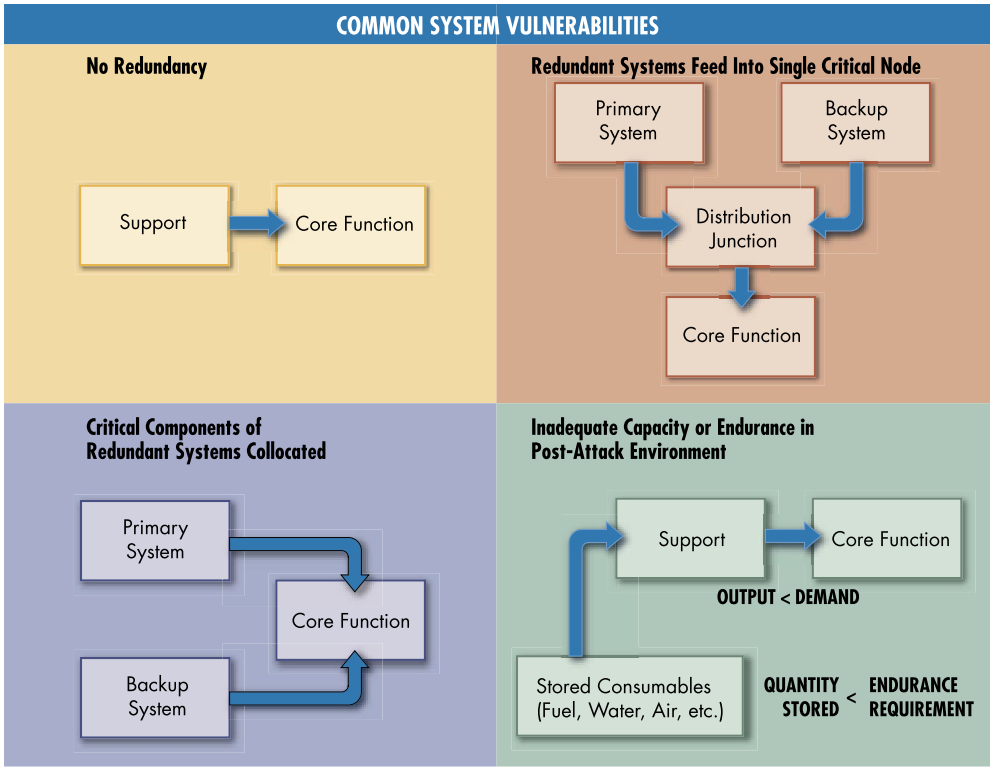

Figure 3-2 Common system vulnerabilities

Scale for Vulnerability Rating

For this How-To Guide, the following scale for vulnerability has been selected. Table 3-4 provides a scale for selecting your vulnerability rating. The scale is a combination of a 7-level linguistic scale and a 10-point numerical scale (10 being the greater threat). The key elements of this scale are the weaknesses of your building and easiness and/or difficulties that the aggressors may face when wishing to generate damage to your building. Also, the loss of operations in case of an attack and the lack of redundancies are considered. Tables 3-5A and 3-5B display a nominal example applying these ratings for an urban multi-story building.

Table 3-4: Vulnerability Rating

Criteria		
Very High	10	Very High – One or more major weaknesses have been identified that make the asset extremely susceptible to an aggressor or hazard. The building lacks redundancies/physical protection and the entire building would be only functional again after a very long period of time after the attack.
High	8-9	High – One or more major weaknesses have been identified that make the asset highly susceptible to an aggressor or hazard. The building has poor redundancies/physical protection and most parts of the building would be only functional again after a long period of time after the attack.
Medium High	7	Medium High – An important weakness has been identified that makes the asset very susceptible to an aggressor or hazard. The building has inadequate redundancies/physical protection and most critical functions would be only operational again after a long period of time after the attack.
Medium	5-6	Medium – A weakness has been identified that makes the asset fairly susceptible to an aggressor or hazard. The building has insufficient redundancies/physical protection and most part of the building would be only functional again after a considerable period of time after the attack.
Medium Low	4	Medium Low – A weakness has been identified that makes the asset somewhat susceptible to an aggressor or hazard. The building has incorporated a fair level of redundancies/physical protection and most critical functions would be only operational again after a considerable period of time after the attack.
Low	2-3	Low – A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor or hazard. The building has incorporated a good level of redundancies/physical protection and the building would be operational within a short period of time after an attack.
Very Low	1	Very Low – No weaknesses exist. The building has incorporated excellent redundancies/physical protection and the building would be operational immediately after an attack.

Table 3-5A: Nominal Example of Vulnerability Rating for a Specific Multi-story Building (Building Function)

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration	7	7	9	9	9
Engineering	4	4	5	6	6
Warehousing	4	8	9	9	9
Data Center	5	4	3	4	4
Food Service	1	4	5	9	9
Security	5	5	10	9	9
Housekeeping	1	3	3	3	3
Day Care	3	9	9	9	9

Table 3-5B: Nominal Example of Vulnerability Rating for a Specific Multi-story Building (Building Infrastructure)

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site	1	7	6	4	4
Architectural	1	9	7	2	2
Structural Systems	1	10	7	2	1
Envelope Systems	1	9	7	2	1
Utility Systems	2	6	2	2	1
Mechanical Systems	1	8	5	9	9
Plumbing and Gas Systems	1	6	3	6	2
Electrical Systems	7	8	6	2	1
Fire Alarm Systems	1	6	8	2	1
IT/Communications Systems	8	6	8	2	1

WORKSHEET 3-1: NOMINAL ASSESSMENT SCHEDULE

Assessment Schedule			
Location	**Team Members**	**Dates**	**Comments**
Building 1 Location:		First On-Site Visit	
		Second On-Site Visit	
		Third On-Site Visit	
Building 2 Location:		First On-Site Visit	
		Second On-Site Visit	
		Third On-Site Visit	
		Fourth On-Site Visit	

Contact Information			
Member	**Phone**	**E-mail**	**Comments**
Main Stakeholder			
Field Staff			
Team Member 1			
Team Member 2			
Team Member 3			

Worksheet 3-1 provides an example of a nominal assessment schedule for two buildings owned by the same stakeholder. It reflects a multi-day assessment with a variable number of Team members. The bottom of the table includes space to write key contact information. Remember that a Team can be contacted to perform assessments for multiple buildings.

WORKSHEET 3-2: ASSESSMENT AGENDA

Infrastructure	Site and Components to be Assessed	Members
Site		
Architectural		
Structural Systems		
Envelope Systems		
Utility Systems		
Mechanical Systems		
Plumbing and Gas Systems		
Electrical Systems		
Fire Alarm Systems		
IT/Communications Systems		

Worksheet 3-2 will help you to prepare your assessment agenda. Using the Building Vulnerability Assessment Checklist, the Team should propose the areas that need to be analyzed during the on-site visits. The proposed list will be discussed with building owners and facility managers and will be finalized by the Assessment Team.

WORKSHEET 3-3: VULNERABILITY RATING

Function	Vulnerability	Infrastructure	Vulnerability
Administration		Site	
Engineering		Architectural	
Warehousing		Structural Systems	
Data Center		Envelope Systems	
Food Service		Utility Systems	
Security		Mechanical Systems	
Housekeeping		Plumbing and Gas Systems	
Day Care		Electrical Systems	
Other		Fire Alarm Systems	
Other		IT/Communications Systems	

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

Worksheet 3-1 can be used to complete your risk assessment and will be used in conjunction with Worksheets 4-1 and 4-2. It can be used to discuss the vulnerability rating with building stakeholders and among the members of the Assessment Team. Vulnerability rating refers to a numerical value that can be assigned to building weaknesses and lack of redundancy.

To fill out Worksheet 3-1, analyze the impact of a particular threat to your site and/or building. Analyze core functions and building infrastructure components as indicated in Task 2.2 of Step 2. Analyze your assets based on: a) the identified threat; b) the criticality of your assets: and c) a level of protection you may have chosen (i.e., your willingness or unwillingness to accept risk). When assigning a vulnerability rating, consider redundancy factors included in Task 3.4. This may increase your vulnerability rating for functions and infrastructure.