OVERVIEW

The fourth step in the assessment process is to prepare a risk assessment for your site and building (see Figure 4-1). The risk assessment analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood of the threat occurring and the consequences of the occurrence.

The risk assessment process involves the following tasks:

- Preparing the risk assessment matrices
- Determining the risk ratings
- Prioritizing observations in the Building Vulnerability Assessment Checklist

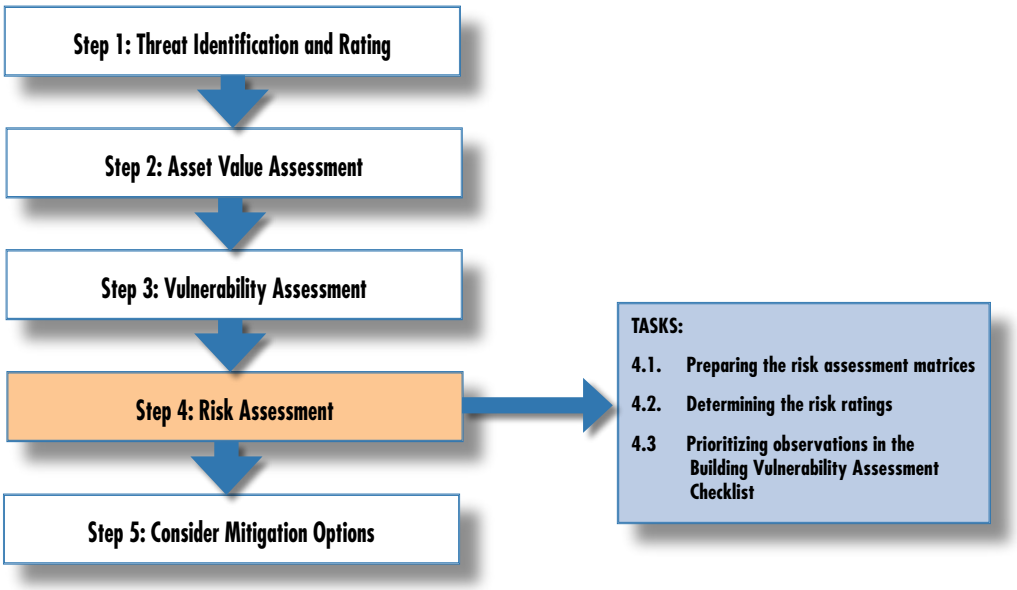

Figure 4-1 Steps and tasks

There are a number of methods and means to conduct a building risk assessment, and the steps can be accomplished in different sequences. However, they all have one common objective, which is to apply a quantitative assessment process that identifies those assets at highest risk and evaluate mitigation measures that can reduce that risk. The process selected for this How-To Guide is described below.

Preparing the Risk Assessment Matrices (Task 4.1)

In order to estimate potential losses, a series of matrices have been prepared. The inputs for these matrices are based on the analysis performed during Steps 1, 2, and 3.

To estimate risk, a number of factors need to be taken into consideration. The first one is to identify and rate the threats that could cause harm to a building and its inhabitants. Next, the value of assets and people that need to be protected will be identified. After threats and assets are identified, a vulnerability rating that identifies weaknesses that might be exploited by a terrorist or aggressor is determined. Risk can be computed using the results of the threat rating, asset value, and vulnerability rating.

Tables 4-1 to 4-10 can be used as a pre-assessment screening tool by the Team while conducting the on-site meetings with key staff members (e.g., building owners, security, site management, key function representatives, etc.). The tables should be completed by consensus judgment of the building stakeholders and Assessment Team members. The risk assessment matrices can provide both a quantitative score and color code to objectively and visually determine the functions and systems that have been determined to be at risk.

During Steps 1 and 2, you should have identified your threat rating (Worksheet 1-2), asset value (Worksheet 2-1), and vulnerability rating (Worksheet 3-3). At this point, you should transfer these values to Worksheets 4-1 and 4-2.

In the risk assessment matrices, the threats are listed across the top, and the functions and infrastructure are listed down the side to create threat-pairs. In general, there are two approaches to complete Worksheets 4-1 and 4-2. One approach is to start with all cell elements set to zero and discuss each element in detail to arrive at a consensus number. Another approach is to start with all cell elements equal to a numeric value (e.g., "5") and then adjust cell values up or down. With either approach, the first few rows and columns will take the longest time to reach consensus values, but, as the group becomes familiar with the ratings and scales, the process converges quickly. It should take approximately 3 to 4 hours to complete the matrices and, during that time, many of the building vulnerabilities will be verbally identified and collaborated with the vulnerability portfolio and earlier building site tour.

Identifying and Determining the Threat Rating. Step 1 will help you to identify and come to a consensus in terms of the threat rating. After each threat/hazard has been identified and defined, the threat level for each

threat/hazard shall be determined. The threat rating is a subjective judgment of a terrorist threat based on existence, capability, history, intentions, and targeting. The threat rating is a snapshot in time, and can be influenced by many factors, but the given threat value will typically be the same for each function (going down the columns). Organizations that are dispersed in a campus environment may have variations in ratings. For threat rating, a scale from 1-10 was assigned: 10 is considered very high; 8-9 is high; 7 is medium high; 5-6 is medium; 4 is medium low; 2-3 is low; and 1 is very low.

Rating the Asset Value. Step 2 will help you to determine the asset value rating for your site and/or building. After a building's assets requiring protection have been identified, they should be assigned a value. The asset value is the degree of debilitating impact that would be caused by the incapacity or destruction of the building's assets. There are a number of methods and means to conduct a building risk assessment, and the steps can be accomplished in different sequences, but the objective is to apply a quantitative assessment process that identifies those assets at highest risk and evaluate mitigation measures that can reduce that risk. For an asset value rating, a scale from 1-10 was assigned: 10 is considered very high; 8-9 is high; 7 is medium high; 5-6 is medium; 4 is medium low; 2-3 is low; and 1 is very low.

Assessing the Vulnerability. Step 3 will help you to determine the vulnerability rating for your site and/or building. After your threat rating and asset value rating have been identified, the vulnerability rating should be determined. Vulnerability rating requires identifying and rating the vulnerability of each asset-threat pair. An indepth vulnerability assessment of a building evaluates specific design and architectural features, and identifies all vulnerabilities of the building functions and building systems. In the vulnerability rating scale of 1 to 10, 1 means very low or no weaknesses exist, and 10 means one or more major weaknesses exist to make an asset extremely susceptible to an aggressor.

Critical Functions Asset Value. Table 4-1 depicts a portion of the site critical functions matrix. It lists the functions down the left side and threats across the top. The asset value rating is entered into the site critical functions matrix and begins the process of quantifying the risk elements. In general, the asset value for a given function is the same for all threats and the matrix helps to identify the primary functions in a quantitative form. The functions matrix is people oriented and subjective, and provides a guide to vulnerabilities and risks. The asset value under the engineering and administration functions is highlighted. For administration, a medium asset value (5) was assigned for

all threats. For engineering, a high asset rating (8) was determined for all threats.

Table 4-1: Critical Functions Asset Value

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration					
Asset Value	5	5	5	5	5
Threat Rating					
Vulnerability Rating					
Engineering					
Asset Value	8	8	8	8	8
Threat Rating					
Vulnerability Rating					

Critical Infrastructure Asset Value. Table 4-2 depicts a portion of the site critical infrastructure matrix. It lists infrastructure down the left side and threats across the top. In general, the asset value for a given infrastructure asset is the same for all threats and is usually the economic cost of replacement. The value can be changed to reflect intangibles such as duration of loss, loss of production capability, etc. The asset value rating under the site and structural systems is highlighted. A medium low asset value rating (4) was assigned for the site infrastructure threat pairs. A high asset value rating (8) was assigned for the structural system threat pairs.

Table 4-2: Critical Infrastructure Asset Value

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site					
Asset Value	4	4	4	4	4
Threat Rating					
Vulnerability Rating					
Structural Systems					
Asset Value	8	8	8	8	8
Threat Rating					
Vulnerability Rating					

Critical Functions Threat Rating. The threat rating under the site and structural systems is highlighted in Table 4-3. A high threat rating (8) was assigned for a cyber attack based on known groups releasing worms and viruses; a medium low threat rating (4) was assigned for a vehicle bomb; a medium threat rating (5) was assigned for a suicide bomber based on current intelligence on known groups and quantity of explosives available; and a low threat rating (2)

was assigned for both Sarin and Ricin attacks based on current intelligence of prior targets and predicted use against future targets (assuming that the building is not the primary target, but may experience collateral damage effects).

Table 4-3: Critical Functions Threat Rating

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration					
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating					
Engineering					
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating					

Critical Infrastructure Threat Rating. The threat rating under the site and structural systems is highlighted in Table 4-4. A high threat rating (8) was assigned for a cyber attack based on known groups releasing worms and viruses; a medium low threat rating (4) was assigned for a vehicle bomb; a medium threat rating (5) was assigned for a suicide bomber based on current intelligence on known groups and quantity of explosives available; and a low threat rating (2) was assigned for both Sarin and Ricin attacks based on current intelligence of prior targets and predicted use against future targets (assuming that the building is not the primary target, but may experience collateral damage effects).

Table 4-4: Critical Infrastructure Threat Rating

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site					
Asset Value	4	4	4	4	4
Threat Rating	8	4	5	2	2
Vulnerability Rating					
Structural Systems					
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating					

Critical Functions Vulnerability Rating. In Table 4-5, for administration, a medium high vulnerability rating (7) was determined for a cyber attack; a medium high vulnerability rating (7) was determined for a vehicle bomb; a

high vulnerability rating (9) was assigned for a suicide bomber, and for Sarin and Ricin attacks because administration is located at the lobby entrance. For engineering, a medium vulnerability rating (7) was determined for a cyber attack; a medium low vulnerability rating (4) was determined for a vehicle bomb; a medium vulnerability rating (5) was determined for a suicide bomber; and a medium vulnerability rating (6) was determined for a Sarin or Ricin attack.

Table 4-5: Critical Functions Vulnerability Rating

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration					
Asset Value	5	5	5	5	5
Threat Rating	8	4	3	2	2
Vulnerability Rating	7	7	9	9	9
Engineering					
Asset Value	8	8	8	8	8
Threat Rating	8	5	6	2	2
Vulnerability Rating	7	4	5	6	6

Critical Infrastructure Vulnerability Rating. In Table 4-6, a low vulnerability rating (1) was determined for a cyber attack because there are no internet devices; a medium high vulnerability rating (7) was determined for a vehicle bomb; a low vulnerability rating (3) was determined for a suicide bomber; a low vulnerability rating (2) for Sarin and Ricin attacks because there would be little damage impact on the site. For structural systems, a low vulnerability rating (1) was determined for a cyber attack; a high vulnerability rating (10) was determined for a vehicle bomb due to progressive collapse concerns; a medium vulnerability rating (6) was determined for a suicide bomber who could place a device next to a primary support and load bearing column; and a low vulnerability rating (1) was determined for a Sarin or Ricin attack because there would be little or no damage.

Table 4-6: Critical Infrastructure Vulnerability Rating

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site					
Asset Value	4	4	4	4	4
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	7	3	2	2
Structural Systems					
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	10	6	1	1

Determining the Risk Ratings (Task 4.2)

Risk is the potential for a loss 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), asset value (consequences of the occurrence), and vulnerabilities to ascertain the level of risk for each asset against each applicable threat/hazard. The risk assessment provides engineers and architects with a relative risk profile that defines which assets are at the greatest risk against specific threats.

There are numerous methodologies and technologies for conducting a risk assessment. For this How-To Guide, the approach is to assemble the results of the threat assessment, asset value 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

To prepare the risk estimation matrices three factors or elements of risk are considered for each function or system against each threat previously identified. Multiplying the values assigned to each of the three factors provides quantification of total risk. The total risk for each function or system against each threat is assigned a color code. The results of the risk assessment should be used to help prioritize which mitigation measures should be adopted, given limited resources, in order to achieve a desired level of protection. To determine your risk rating, you may use Table 4-7, which includes information on observations in the Building Vulnerability Assessment Checklist (Appendix A) on the total risk scale and color codes. A site functional pre-screening matrix is shown in Table 4-8 and a site infrastructure pre-screening matrix is

shown in Table 4-9. Worksheets 4-1 and 4-2 will assist you in preparing and organizing the information for your risk assessment.

Table 4-7: Total Risk Scale Color Code

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

Table 4-8: Site Functional Pre-Assessment Screening Matrix

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration	280	140	225	90	90
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	7	9	9	9
Engineering	448	128	200	96	96
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	4	5	6	6
Warehousing	168	96	135	54	54
Asset Value	3	3	3	3	3
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	8	9	9	9
Data Center	320	128	120	64	64
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	5	4	3	4	4
Food Service	112	32	50	36	36
Asset Value	2	2	2	2	2
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	4	5	9	9
Security	392	140	350	126	126
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	5	10	9	9
Housekeeping	112	24	30	12	12
Asset Value	2	2	2	2	2
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	3	3	3	3
Day Care	504	324	405	162	162
Asset Value	9	9	9	9	9
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	9	9	9	9

Table 4-9: Site Infrastructure Pre-Assessment Screening Matrix

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site	32	128	60	16	16
Asset Value	4	4	4	4	4
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	7	3	4	4
Architectural	40	180	175	20	20
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	9	7	2	2
Structural Systems	64	320	240	32	32
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	10	6	2	1
Envelope Systems	56	252	210	28	14
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	9	6	2	1
Utility Systems	112	168	70	28	14
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	2	6	2	2	1
Mechanical Systems	56	224	175	126	126
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	8	5	9	9
Plumbing and Gas Systems	40	120	75	60	20
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	6	3	6	2
Electrical Systems	392	224	210	28	14
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	8	6	2	1
Fire Alarm Systems	72	216	320	36	18
Asset Value	9	9	9	9	9
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	6	8	2	1
IT/Communications Systems	512	192	240	32	16
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	8	6	6	2	1

Prioritizing Observations in the Building Vulnerability Assessment Checklist (Task 4.3)

The Building Vulnerability Assessment Checklist relates to building core infrastructure. During Task 3.3, the Assessment Team performed an on-site assessment and filled out observations in the Building Vulnerability Assessment Checklist. (Table 4-10 provides a nominal example.) As mentioned before, the Checklist is a key tool in the preparation of the vulnerability assessment. It is used to guide the assessors performing the assessment of the facility. The vulnerabilities of the facility are selected from the observations provided for each vulnerability question. These vulnerabilities are then prioritized to determine the most effective mitigation measures. Prioritization is based on the greatest vulnerabilities that can be exploited by the aggressors and largest risks in terms of loss of lives, building damage, and loss of operation. Task 4.3 is the final task of the risk assessment. It allows the assessors to rank their observed facility vulnerabilities and proposed remedial actions. Worksheet 4-3 will help you to perform this task. For more information on how to use the Building Vulnerability Assessment Checklist, see Step 3 and Appendix A.

Table 4-10: Nominal Example of Observations in the Building Vulnerability Assessment Checklist

Section	Vulnerability Question	Guidance	Observations
1.	**Site**		
	Is a perimeter fence or other types of barrier controls in place?	The intent is to channel pedestrian traffic onto a site with multiple buildings through known access control points. For a single building, the intent is to have a single visitor entrance. Reference: *GSA PBS-P100*	The main gate entrance remains wide open for vehicle and pedestrian intruders. There are missing street signs throughout the facility. It is difficult to channel staff and visitors to control access points. There is only one security vehicles to serve the entire campus; at least two more are required.
2.	**Architectural**		
2.27	**Is interior glazing near high-risk areas minimized?** **Is interior glazing in other areas shatter-resistant?**	Interior glazing should be minimized where a threat exists and should be avoided in enclosures of critical functions next to high-risk areas. Reference: *GSA PBS-P100*	In the main facade, windows are not blast-resistant and the glass is not properly anchored to the frame. In case of a blast event, it is anticipated that the glass will break and will not remain in the frame. This could cause extensive injuries in case of an explosive event.
8.	**Utility Systems**		
8.6	**Does emergency backup power exist for all areas within the building or for critical areas only?** **How is the emergency power distributed?** **Is the emergency power system independent from the normal electrical service, particularly in critical areas?**	There should be no single critical node that allows both the normal electrical service and the emergency backup power to be affected by a single incident. Automatic transfer switches and interconnecting switchgear are the initial concerns. Emergency and normal electrical equipment should be installed separately, at different locations, and as far apart as possible. Reference: *GSA PBS-P100*	There are single-point vulnerabilities to the steam and electricity lines. Any damage to the steam or electric lines would result in loss of utilities.

WORKSHEET 4-1: SITE FUNCTIONAL PRE-ASSESSMENT MATRIX

Worksheet 4-1 can be used to complete your risk assessment by determining the functions at a higher risk. To fill out this matrix, use the scales and color codes, provided in Steps 4.1 and 4.2 .

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

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration					
Asset Value					
Threat Rating					
Vulnerability Rating					
Engineering					
Asset Value					
Threat Rating					
Vulnerability Rating					
Warehousing					
Asset Value					
Threat Rating					
Vulnerability Rating					
Data Center					
Asset Value					
Threat Rating					
Vulnerability Rating					
Food Service					
Asset Value					
Threat Rating					
Vulnerability Rating					
Security					
Asset Value					
Threat Rating					
Vulnerability Rating					
Housekeeping					
Asset Value					
Threat Rating					
Vulnerability Rating					
Day Care					
Asset Value					
Threat Rating					
Vulnerability Rating					

WORKSHEET 4-2: SITE INFRASTRUCTURE SYSTEMS PRE-ASSESSMENT MATRIX

Worksheet 4-2 can be used to complete your risk assessment by determining the infrastructure at a higher risk.

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site					
Asset Value					
Threat Rating					
Vulnerability Rating					
Architectural					
Asset Value					
Threat Rating					
Vulnerability Rating					
Structural Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Envelope Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Utility Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Mechanical Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Plumbing and Gas Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Electrical Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Fire Alarm Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
IT/Communications Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					

WORKSHEET 4-3: PRIORITIZATION OF OBSERVATIONS IN THE CHECKLIST

The observations you made in the Building Vulnerability Checklist (Appendix A) during Step 3 should now be used to review the vulnerability ratings in Worksheets 4-1 and 4-2, and then the risk ratings for the associated Threat-Asset Pairs in those worksheets. The observations that you use to confirm or adjust the vulnerability ratings are your selected vulnerabilities that Worksheet 4-3 can help you prioritize. The top portion of Worksheet 4-3 should have the selected observations/vulnerabilities listed in the Cross Reference Column. Using the updated results of Worksheets 4-1 and 4-2, indicate all high risk (red) Functions and Infrastructure column-row intersections that the vulnerability in the Cross Reference Column impacts. As previously stated, prioritization is based on the greatest vulnerabilities that can be exploited by the aggressors and largest risks in terms of loss of lives, building damage, and loss of operation. The bottom portion of Worksheet 4-3 should contain your selected observations/vulnerabilities that meet this statement in rank order – highest to lowest. For example, Ranked Observation 1 would have the highest vulnerability rating matched with the highest risk rating and impacting the greatest number of Functions and Infrastructure. This table can be expanded to include more observations, as needed. In the Risk Assessment Database, vulnerabilities can be given a priority of 1 to 5 as defined by the Manager prior to the assessment. For example, the priority could be based upon the speed in which the vulnerability should be mitigated, or needed level of risk reduction sought, or ability to be exploited by the aggressor, etc.

Cross Reference	Functions	Administration	Engineering	Warehousing	Data Center	Food Service	Security	Housekeeping	Day Care	Infrastructure	Site	Architectural	Structural Systems	Envelope Systems	Utility Systems	Mechanical Systems	Plumbing and Gas Systems	Electrical Systems	Fire Alarm Systems	IT/Communications Systems
Observation 1																				
Observation 2																				
Observation 3																				
Observation 4																				
Observation 5																				
Observation 6																				
Ranked Observations																				
Observation 1																				
Observation 2																				
Observation 3																				
Observation 4																				
Observation 5																				
Observation 6																				