Basic Element	Points to Consider
1. Characterization of the water system, including its mission and objectives. (Answers to system-specific questions may be helpful in characterizing the water system.)	• What are the important missions of the system to be assessed? Define the highest priority services provided by the utility. Identify the utility's customers: < General public < Government < Military < Industrial < Critical care < Retail operations < Firefighting • What are the most important facilities, processes, and assets of the system for achieving the mission objectives and avoiding undesired consequences? Describe the: < Utility facilities < Operating procedures < Management practices that are necessary to achieve the mission objectives < How the utility operates (e.g., water source including ground and surface water) < Treatment processes < Storage methods and capacity < Chemical use and storage < Distribution system In assessing those assets that are critical, consider critical customers, dependence on other infrastructures (e.g., electricity, transportation, other water utilities), contractual obligations, single points of failure (e.g., critical aqueducts, transmission systems, aquifers etc.), chemical hazards and other aspects of the utility's operations, or availability of other utility capabilities that may increase or decrease the criticality of specific facilities, processes and assets.

Basic Element	Points to Consider
2. Identification and prioritization of adverse consequences to avoid.	• Take into account the impacts that could substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water or otherwise present significant public health concerns to the surrounding community. Water systems should use the vulnerability assessment process to determine how to reduce risks associated with the consequences of significant concern. • Ranges of consequences or impacts for each of these events should be identified and defined. Factors to be considered in assessing the consequences may include: < Magnitude of service disruption < Economic impact (such as replacement and installation costs for damaged critical assets or loss of revenue due to service outage) < Number of illnesses or deaths resulting from an event < Impact on public confidence in the water supply < Chronic problems arising from specific events < Other indicators of the impact of each event as determined by the water utility. Risk reduction recommendations at the conclusion of the vulnerability assessment should strive to prevent or reduce each of these consequences.

Basic Element	Points to Consider
3. Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences.	• What are the malevolent acts that could reasonably cause undesired consequences? Consider the operation of critical facilities, assets and/or processes and assess what an adversary could do to disrupt these operations. Such acts may include physical damage to or destruction of critical assets, contamination of water, intentional release of stored chemicals, interruption of electricity or other infrastructure interdependencies. • The "Public Health Security and Bioterrorism Preparedness and Response Act of 2002" (PL 107-188) states that a community water system which serves a population of greater than 3,300 people must review the vulnerability of its system to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. The vulnerability assessment shall include, but not be limited to, a review of: < Pipes and constructed conveyances < Physical barriers < Water collection, pretreatment and treatment facilities < Storage and distribution facilities < Electronic, computer or other automated systems which are utilized by the public water system (e.g., Supervisory Control and Data Acquisition (SCADA)) < The use, storage, or handling of various chemicals < The operation and maintenance of such systems

Basic Element	Points to Consider
4. Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries (e.g., terrorists, vandals).	• Determine the possible modes of attack that might result in consequences of significant concern based on the critical assets of the water system. The objective of this step of the assessment is to move beyond what is merely possible and determine the likelihood of a particular attack scenario. This is a very difficult task as there is often insufficient information to determine the likelihood of a particular event with any degree of certainty. • The threats (the kind of adversary and the mode of attack) selected for consideration during a vulnerability assessment will dictate, to a great extent, the risk reduction measures that should be designed to counter the threat(s). Some vulnerability assessment methodologies refer to this as a "Design Basis Threat" (DBT) where the threat serves as the basis for the design of countermeasures, as well as the benchmark against which vulnerabilities are assessed. It should be noted that there is no single DBT or threat profile for all water systems in the United States. Differences in geographic location, size of the utility, previous attacks in the local area and many other factors will influence the threat(s) that water systems should consider in their assessments. Water systems should consult with the local FBI and/or other law enforcement agencies, public officials, and others to determine the threats upon which their risk reduction measures should be based. Water systems should also refer to EPA's "Baseline Threat Information for Vulnerability Assessments of Community Water Systems" to help assess the most likely threats to their system. This document is available to community water systems serving populations greater than 3,300 people. If your system has not yet received instructions on how to receive a copy of this document, then contact your Regional EPA Office immediately. You will be sent instructions on how to securely access the document via the Water Information Sharing and Analysis Center (ISAC) website or obtain a hardcopy that can be mailed directly to you. Water systems may also want to review their incident reports to better understand past breaches of security.

Basic Element	Points to Consider
5. Evaluation of existing countermeasures. (Depending on countermeasures already in place, some critical assets may already be sufficiently protected. This step will aid in identification of the areas of greatest concern, and help to focus priorities for risk reduction.)	• *What capabilities does the system currently employ for detection, delay and response?* < Identify and evaluate current detection capabilities such as intrusion detection systems, water quality monitoring, operational alarms, guard post orders, and employee security awareness programs. < Identify current delay mechanisms such as locks and key control, fencing, structure integrity of critical assets and vehicle access checkpoints. < Identify existing policies and procedures for evaluation and response to intrusion and system malfunction alarms, adverse water quality indicators, and cyber system intrusions. **It is important to determine the performance characteristics. Poorly operated and maintained security technologies provide little or no protection.** • *What cyber protection system features does the utility have in place?* Assess what protective measures are in-place for the SCADA and business-related computer information systems such as: < Firewalls < Modem access < Internet and other external connections, including wireless data and voice communications < Security policies and protocols **It is important to identify whether vendors have access rights and/or "backdoors" to conduct system diagnostics remotely.** • *What security policies and procedures exist, and what is the compliance record for them?* Identify existing policies and procedures concerning: < Personnel security < Physical security < Key and access badge control < Control of system configuration and operational data < Chemical and other vendor deliveries < Security training and exercise records

Basic Element	Points to Consider
6. Analysis of current risk and development of a prioritized plan for risk reduction.	• Information gathered on threat, critical assets, water utility operations, consequences, and existing countermeasures should be analyzed to determine the current level of risk. The utility should then determine whether current risks are acceptable or risk reduction measures should be pursued. • Recommended actions should measurably reduce risks by reducing vulnerabilities and/or consequences through improved deterrence, delay, detection, and/or response capabilities or by improving operational policies or procedures. Selection of specific risk reduction actions should be completed prior to considering the cost of the recommended action(s). Utilities should carefully consider both short- and long-term solutions. An analysis of the cost of short- and long-term risk reduction actions may impact which actions the utility chooses to achieve its security goals. • Utilities may also want to consider security improvements in light of other planned or needed improvements. Security and general infrastructure may provide significant multiple benefits. For example, improved treatment processes or system redundancies can both reduce vulnerabilities and enhance day-to-day operation. • Generally, strategies for reducing vulnerabilities fall into three broad categories: < Sound business practices – affect policies, procedures, and training to improve the overall security-related culture at the drinking water facility. For example, it is important to ensure rapid communication capabilities exist between public health authorities and local law enforcement and emergency responders. < System upgrades – include changes in operations, equipment, processes, or infrastructure itself that make the system fundamentally safer. < Security upgrades – improve capabilities for detection, delay, or response.