

Order Number 940A

The Importance of Risk Management in Site Preparation

Traditional facility security measures such as perimeter fences, access gates, or surveillance cameras are designed to keep potential threats out of a facility and its sensitive areas. However, under current and emerging arms control treaties, foreign inspection teams are allowed to pass through traditional security measures and conduct certain inspection activities throughout an inspected facility. Thus, U.S. Government, defense contractor, and private industry facilities susceptible to these on-site inspections and observation flights may be required to modify or create new methods for protecting national security, proprietary, and other sensitive information.

Risk management is a useful and important process for developing appropriate security countermeasures at facilities subject to intrusive arms control activities. By incorporating risk management into site preparation activities, facility staffs are able to locate, identify, and protect sensitive information in a cost-effective manner. Without the application of this process, sensitive information may be inadvertently disclosed or safety and security standards could be compromised.

Risk Management—An Overview

Simply defined, “risk” measures the likelihood or probability that an undesirable event could occur (i.e. an event potentially causing harm to an important aspect of a facility). Risk management is a systematic process designed to help facility staffs develop rational and cost-effective security countermeasures. The process considers both short- and long-term monetary and non-monetary costs. By including a cost-benefit analysis in the risk management process, new procedures or methods implemented to mitigate risk tend to be more uniform and efficient.

Like the operations security (OPSEC) process, risk management entails the assessment of assets, threats, and vulnerabilities to collectively target and mitigate particular facility concerns. However, risk

management differs from OPSEC in that it focuses on a wide range of sensitive assets, whereas OPSEC focuses more narrowly on indicators of sensitive information. Whether employed separately or as part of the OPSEC process, risk management promotes the implementation of cost-effective, appropriate security countermeasures tailored to the level of risk facility managers are willing to accept.

Risk management is most important during site preparation activities, when facility staffs conduct specific readiness activities and comprehensively examine the facility to evaluate its readiness to host arms control inspections. During site preparation planning, staffs agree on procedures enabling them to demonstrate compliance with U.S. treaty obligations while simultaneously protecting national security, proprietary, or other sensitive information. Facility security concerns become apparent as exposed programs, program information, or other sensitive indicators are identified.

Risk Management—The Process

The first step of the OPSEC process identifies sensitive indicators. These indicators will be included as assets for further assessment under risk management. Risk management is a process consisting of six steps:

1. Assess assets
2. Assess threats
3. Assess vulnerabilities
4. Assess risks
5. Prioritize countermeasure options
6. Make risk management decisions

Together, these steps enable facility staffs to conduct a cost-benefit analysis prior to discussing possible countermeasure options. The necessity for additional security measures is countered with specific countermeasures tailored to particular facility concerns. Countermeasures developed through this process either deter, control, or deny possible breaches of security or the compromise of sensitive information.

1. Assess assets

The first step of the risk management process, asset identification and assessment, is designed to locate

and identify assets, and to determine the potential impact associated with having foreign inspection teams acquire information about these assets. Assets may include people, programs, reputation, capabilities, or intellectual property. To perform a sufficient asset survey, facility staffs need to identify sensitive activities and information, the personnel involved, and the specific locations of identified assets, as well as any expected impacts resulting from these assets being compromised.

Once an asset is identified, extensive analysis is required to determine its value. Facility staffs need to determine what the facility stands to lose or gain by protecting the asset, the value of the asset outside the facility's control, the cost of the asset's development and, most important, any impact the asset's disclosure would have on national security or proprietary interests. Additionally, facility staffs need to understand how the potential acquisition of a particular asset could help adversaries attain any goals they may have. Identifying adversaries or competitors is a key consideration in the risk assessment process.

2. Assess threats

Threat assessment assumes special significance for arms control activities and, more important, site preparation. A threat is any indication, circumstance, or event with the potential to cause loss or damage to an asset. Facility staffs face a potential threat from inspectors who are granted access to their facility for the expressed purpose of collecting data to verify a State Party's compliance with a particular arms control agreement. Understanding this threat requires an assessment of the intent or motivations of the inspectors, their capabilities, and any historical actions pertinent to the facility's inspection concerns.

Due to the unique nature and requirements of each asset, a threat estimate needs to be prepared for each one. Although risk management also considers hostile threats—such as the destruction or loss of an asset, operational disruptions, or character attacks—it also protects against the inadvertent disclosure of sensitive information to inspectors. Therefore, the main threat for which facility staffs need to be prepared is the collection of information rather than the destruction or defamation of an asset. The risk management process can help provide protection.

3. Assess vulnerabilities

Once facility staffs have identified which assets should be protected and who they should be protected from, it is time to assess vulnerabilities. A vulnerability is a weakness that could be exploited, possibly resulting in the compromise of assets. Vulnerabilities during arms control activities can be categorized as physical, technical, or operational. Physical vulnerabilities may include building design, facility perimeter security, or geographical information. Technical vulnerabilities include equipment characteristics and systems or telecommunication networks. Operational vulnerabilities include personnel behavior, procedures, or existing security methodologies. A breach of any one of these vulnerabilities could result in assets being compromised. Therefore, vulnerabilities need to be identified and addressed prior to the arrival of the inspection team (i.e. during site preparation activities).

The level of vulnerability for each asset is determined by assessing the weaknesses that make it vulnerable, the likelihood of the vulnerability being exploited, and the effectiveness of any existing security measures (i.e. what, precisely, are they designed to protect). Many facilities unfamiliar with arms control activities do not operate security practices designed to meet the challenges of on-site inspections and observation flights. Therefore, it is important for facility staffs to examine each vulnerability and any protective measures currently in place.

4. Assess risks

After evaluating the assets, threats, and vulnerabilities, facility staffs can assess the actual risks. To do so, the degree of impact needs to be calculated relative to each asset. Assets then need to be prioritized in order of importance, while the likelihood of a specific vulnerability being exploited needs to be estimated. The goal of this step is to identify and evaluate the level of risk associated with the assets being considered. The level of risk will vary according to the asset.

Like the threat assessment step, risk assessment needs to incorporate the presence of the inspector when considering site preparation activities. The skills, abilities, and verification tools at the disposal of inspection teams have a significant effect on the overall risk a facility faces during inspection activities. For example, inspection teams from the Organization for the Prohibition of Chemical Weapons (OPCW)—the Convention's

implementation body—have the right to have samples taken and to analyze them. They also have the right to have photographs taken and to review pertinent facility records. These rights need to be considered when estimating the likelihood of specific vulnerabilities being exploited. The degree of risk can only be determined after incorporating the specific nuances of arms control activities.

The risk formula used to complete the equation is:

$$\text{Risk} = \text{Impact} \times \text{Probability}$$

Where:

- Impact = Expected detrimental impact (asset value; i.e. What would a facility lose? What would an adversary or competitor gain?)
- Probability = Threat (e.g. intelligence collection) x Vulnerability (e.g. perimeter security)

Once each risk is determined, a prioritized list may be created. This list should either be completed during site preparation activities or, for certain facilities, well in advance of a potential inspection to assure that scarce resources are put to the most efficient use.

Examples of undesirable events that could potentially assume special significance during arms control activities include: disruptions to training operations, disruptions to communications, exposing affiliations, exposing protected programs, and the theft or compromise of sensitive information and technologies. Each of these risks may be given a priority-rank numerical rating based on our risk management process. Only then should facility staffs begin to determine whether a particular activity's risks are acceptable or whether adjustments in security methodologies are feasible.

5. Prioritize countermeasure options

The next step is to identify and prioritize countermeasure options. The feasibility, and consequently the appropriateness, of a countermeasure depends on its effectiveness and cost.

The costs associated with each countermeasure include a number of factors such as its purchase or development price, maintenance costs, and life expectancy. The costs of sustaining a countermeasure include staff/contractor salaries for implementation, monitoring, or operational training. In addition to monetary costs, there are costs associated with inconvenience, time, personnel,

and potential delays affecting programs and operational schedules or deployments. When facility staffs determine that an arms control event will increase program security costs beyond what is normally required to protect sensitive information, it is recommended that the program sponsor be consulted before implementing additional security countermeasures.

6. Make risk management decisions

The final step is to make risk management decisions about the appropriate level of protection for each individual asset. It is important to remember that implementing countermeasures tailored to specific assets and vulnerabilities is far more effective during arms control activities than seeking to implement all-encompassing countermeasures.

Remember, too, that the decision to implement countermeasures is not the only possible result of a thorough risk management analysis. Facility staffs may decide to accept a given risk and to apply countermeasures to another, more immediate, concern. Risk acceptance—the informed decision to accept the likelihood and consequences of a particular risk—is a valid conclusion of the risk management process.

Conclusion

Since the specific threat facility staffs will need to address during site preparation activities will not be known until notification of an impending inspection or observation flight is actually received, the risk management process for specific threats will have to be conducted with relatively short notice. However, facility staffs should not wait for such notification before carefully assessing and prioritizing the facility's assets and security countermeasure options. By understanding what the facility's most important assets are, facility staffs will be able to implement overall security programs more efficiently and will be able to carry out site preparation activities with more confidence and expedience.

For additional information about arms control treaties and the application of security countermeasures, contact the DTIRP Outreach Program Coordinator at 800-419-2899 or by email at dtirpoutreach@dtra.mil, your local Defense Security Service (DSS) Industrial Security Representative, or your government sponsor.