Physical Security Office

Risk Based Methodology

For Physical Security Assessments

Why conduct Assessments?

Homeland Security Presidential Directive 7 requires Federal Departments and Agencies identify and prioritize critical infrastructure and key resources and protect them from terrorist attacks.

Homeland Security Presidential Directive 9 requires USDA expand and continue vulnerability assessments of the agriculture and food sectors and update assessments every two (2) years.

Not all assets at all locations require the same degree of protection. Protection of assets must be based on a realistic assessment of the risks associated with the criminal and terrorist threats likely to be directed at the assets in their actual locations.

The Risk Based Methodology for Physical Security Assessments allows leadership to establish asset protection appropriate for the asset(s) value and the likelihood of an attempt to compromise the asset(s).

Leadership can then prioritize assets and apply physical security resources in the most efficient and cost effective manner possible.

The Model - Example

There is a facility that involves GMO research **(Asset).** History shows there is a group of Extremists – **(Threat)** that do not like this type of research. History also indicates their Modus Operandi is to destroy (burn/slash) the unprotected asset **(Vulnerability)** that would **set back research and cost thousands of dollars and hundreds of man-hours to recapture the research (Risk Analysis).** We look at the mission criticality of the asset and the most critical time of risk **(Criticality Assessment)** which is during growing season. Now we look at present protective measures and what is needed **(Gap Analysis)** to protect the asset. We set up our concentric rings of security **(Countermeasures)** starting from the asset working out toward the perimeter. Once the CMs are implemented, a **Training** session on each CM takes place. Now **Test** the CMs, and write an **After Action** report identifying any **Vulnerabilities** in the CMs. Correct the vulnerabilities and test again, until you are satisfied the CMs are adequate to protect against the threat.

Risk Based Methodology for Physical Security Assessments

INTRODUCTION

Risk management is a technical procedure for identifying and evaluating security threats and vulnerabilities and for providing management with options and resource requirements for mitigating the risk(s).

The USDA risk management methodology consists of two distinct phases:

- Assessment phase
  Identifies assets and their criticality
  Identifies specific threats and the probability of occurrence
  Identifies vulnerabilities
  Identifies security countermeasures to mitigate vulnerabilities and protect assets

- Risk evaluation phase – Based on the severity and likelihood of criminal and terrorist attacks and consideration of countermeasures currently in place, this phase estimates the impact of the loss of a critical asset.

These phases are analyzed by a team of multi-disciplined (subject matter) experts who utilize a structured brain-storming technique - known as risk scenario analysis - to develop scenarios and estimate severity of consequences and probability of occurrence. Once estimated, the team uses matrixes to calculate probabilities and vulnerability levels.

Depending on project scope, an assessment may require 2-3 days for data reviews, structured interviews, risk evaluation, and an out briefing.

Risk Based Methodology for Physical Security Assessments

TEAM COMPOSITION

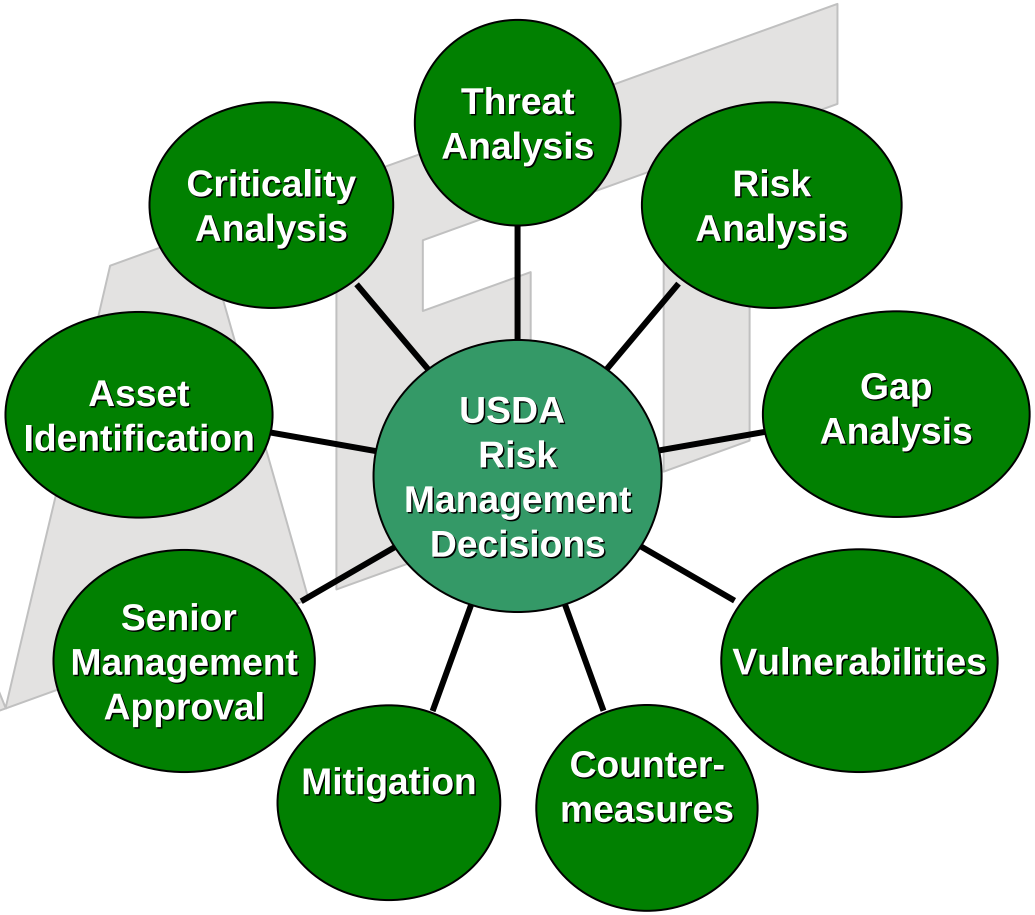
Careful team selection is key to the success of risk assessments. Team composition is flexible and based on the site mission, size, assets, concerns of on-site staff, and the skill sets required of team members. For example, a laboratory assessment at a minimum will include a team member that is a subject matter expert in chemical, radiological, and biological skills, and a physical security specialist team member. For each assessment, an owner must be designated to manage both pre- and post-assessment activities.

SCHEDULING RISK ASSESSMENTS

Risk Management experts should plan and schedule risk assessments. The process may be triggered by schedule, new projects, significant change in a project, occurrence of a serious incident, or when new threat scenarios are identified.

Risk Based Methodology for Physical Security Assessments

The Process very dynamic depending on World and local events



The Risk Assessment Process – Figure 1

Risk Based Methodology for Physical Security Assessments

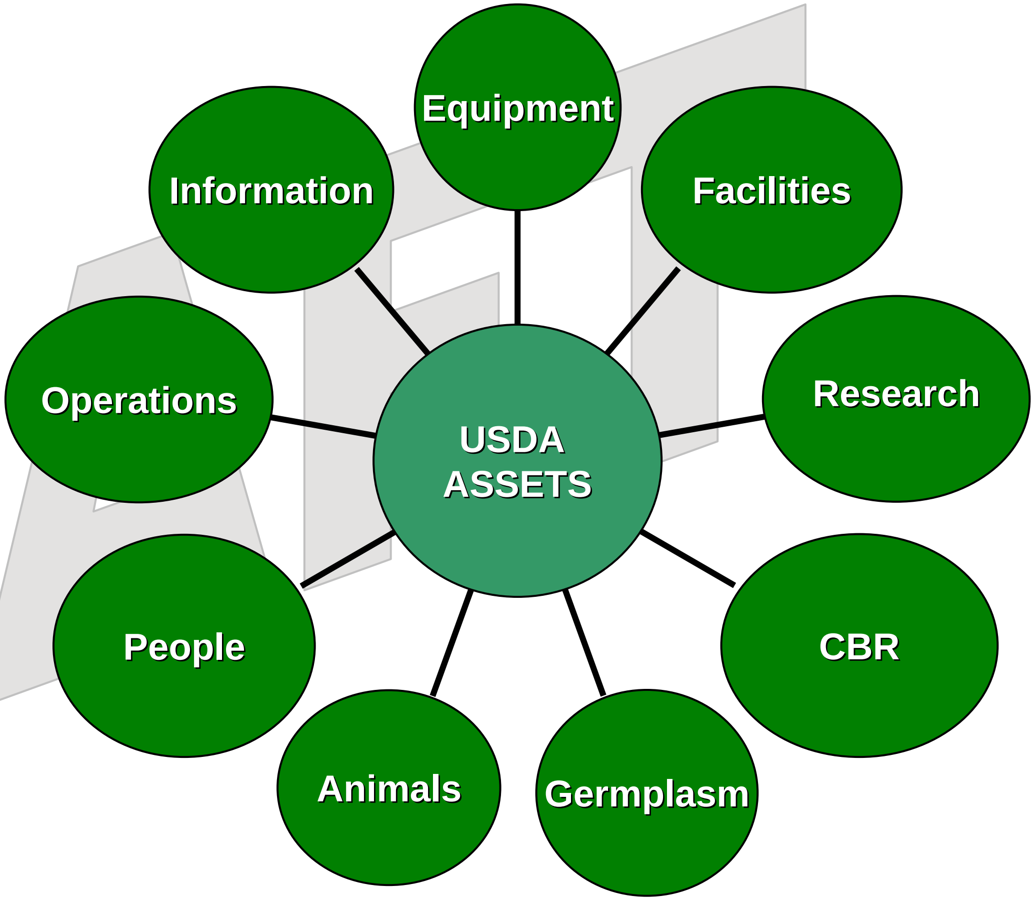
Ranking of Assets for Physical Security Assessments

Assets must be protected because

- If damaged or destroyed could disrupt mission critical work

- If stolen or diverted could pose a threat to public safety

- If damaged or destroyed may be cost prohibitive to replace or irreplaceable



Asset Identification – Figure 2

THE QUALITATIVE RISK ASSESSMENT PROCESS

The Risk Assessment Process is comprised of eight steps which make up the assessment and evaluation phases.

Step 1 - Management Approval, Planning, and Preparation

Management generally approves scheduling and conducting a risk assessment. Management support is vital to the success of the risk assessment process. Management should be involved in determining the scope of the analysis and in the review process. The risk assessment team leader develops the risk assessment plan which identifies team members, scope of work, relevant information, data requirements, key interviewees (generally mid-level managers), schedule, logistics and costs.

Step 2 - Identification of Critical Assets (Resources) Requiring Protection

Critical assets (resources) that need to be protected must be identified. Critical assets may include but are not limited to people, activities/operations, pathogens, chemicals, biologicals, Information, research and equipment. Once assets are identified, then the value or the importance of the asset must be identified.

It is crucial that the team focus on the critical assets to keep the analysis from becoming distracted by an endless discussion of insignificant detail.

Risk Based Methodology for Physical Security Assessments

Therefore, narrow the focus of the assessment to where the most critical assets are located and begin the assessment at that point.

The critical assets should be traced throughout the entire system; there should be a focus on the "totality of activity."

By examining totality, the team will begin to understand relationship's where vulnerabilities may reside and begin the process of scenario development. It is important to note that the asset may have a value to an adversary that is different from its value to an organization.

The team should ask the following questions when determining critical assets:

1. What critical activities and processes take place within the organization?
2. What are the activities of personnel, tenants, customers, and visitors?
3. What material needs are required to complete the mission, and if compromised would prevent mission accomplishment and/or damage to the environment and/or population?
4. When is the asset most vulnerable (crops during growing season, not winter)?
5. What is the critical and sensitive information (any intellectual property, etc.)?
6. What is the critical/valuable equipment (both in cost and mission accomplishment)?
7. What MEVAs support the identified assets (backup generators, distilled water, etc.)?
8. Where are the assets located (is this location the right place and how secure is it)?
9. What are the impacts, if the asset is compromised? (humans, crops, environment, infrastructure, etc.)
10. On a scale ranked from catastrophic to negligible, what is the ranking of the compromised asset?

Risk Based Methodology for Physical Security Assessments

Step 3 - Threats Analysis

This step identifies the specific threats for assets previously identified. An analysis of threat information is critical to the risk assessment process.

As depicted in Figure 3, the threat should be evaluated in terms of insider, outsider, and system induced (that is, organizational or operational flaws).

Threat, similar to assets, should be ranked in terms of likely, possible, remote, and improbable. See table one for definitions. To arrive at this, ask:

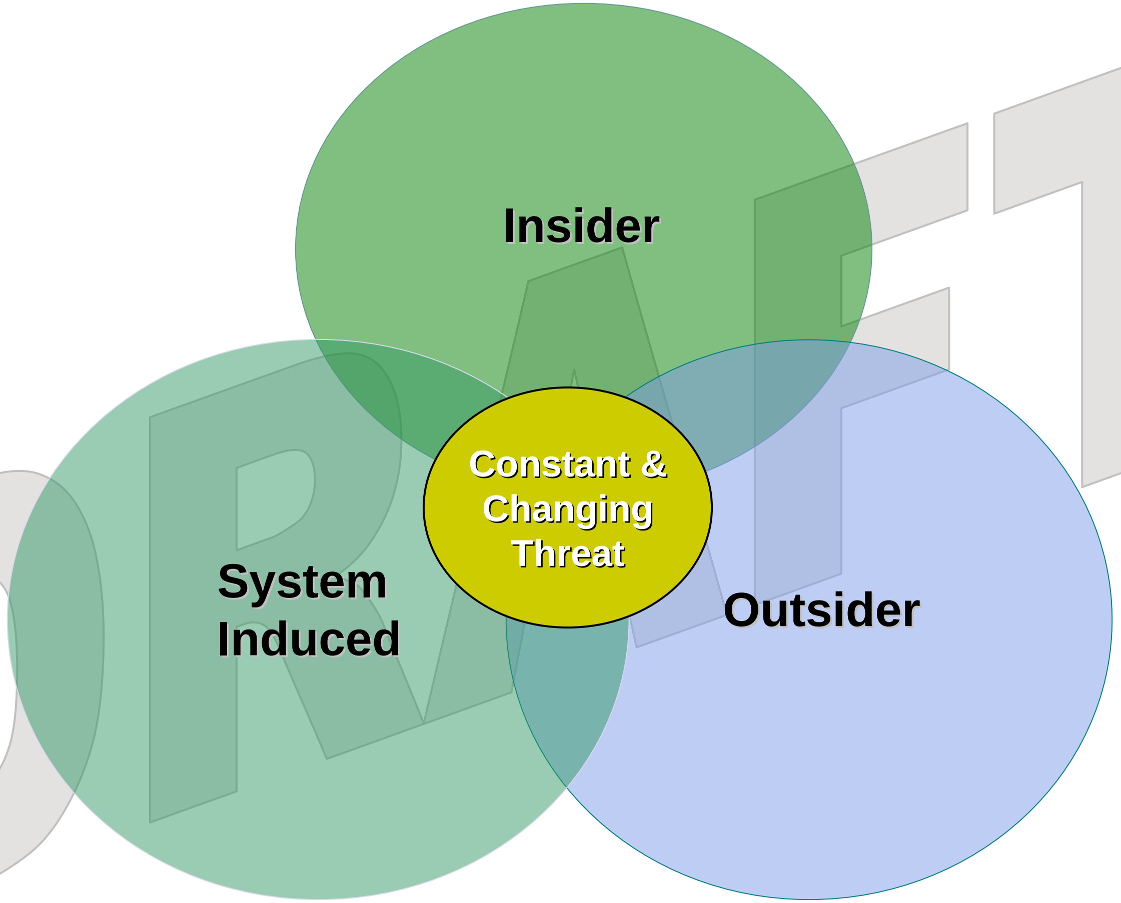
1. What are the goals and objectives of the threat adversary and what does the adversary gain by achieving these goals? How will the adversary achieve these goals? (Earth Liberation Front – keep human intervention out of the environment. Their method of operation, as one example, is to set fire bombs at identified Forest Service buildings)
2. What is the probability of the adversary choosing one method of attack over another method? Is there an easily identified vulnerability that will draw the adversary's attention.
3. What events might provoke a threat?
4. What is the capability of the adversary?
5. What organizational flaws create threat or can be exploited by adversaries? Examples of flaws would be vulnerabilities such as no firewalls on main computer servers that could allow hackers into the server to exploit the information contained inside.

Risk Based Methodology for Physical Security Assessments

Once complete, the threats (adversaries) should be paired with assets to develop an understanding of potential vulnerabilities to the asset. This will facilitate final scenario development.

Types of Threat [Examples]:

1. Indigenous – A specific threat to assets (groups opposed to animal research, genetically modified organisms, roadless issue, etc.)
2. Domestic – Groups opposed to government intervention.
3. International – Fanatics that would attempt to compromise such things as chemical wastes to contaminate water supplies, steal aircraft and run them into major critical infrastructures such as dams, buildings, etc.
4. Criminal Groups – These people are usually perpetrating theft to gain financial reward to support their life style.
5. Vandalism
6. Disgruntled Employee – Someone that is not happy with a specific office and will use internal measures to perpetrate a crime to the asset.



Identification of Threat – Figure 3

Step 4 – Gap Analysis

The “Gap” is the difference between the present asset protection level and the protection level required after a risk and threat analyses have been completed.

1. Once the asset and its characteristics have been identified, and the type of threat(s) that would most likely attempt a compromise to the asset has been identified, one must then look at the protection level and it’s elements necessary to protect the asset. Protection elements are usually in the form of procedures and/or technology.

2. As an example, We have valuable assets (electronic scales) in a lab, there is a threat (criminal), and there are no protection levels for the asset.

3. The “Gap” would be the difference (no protection elements) and the recommended protection level (procedure to lock the laboratory when not occupied and a locking device available to secure the room) to protect the asset.

4. If there are no protection elements to secure these high dollar value assets, then we would need to invoke procedures and purchase and install a locking system.

Step 5 - Analysis of Vulnerability (Scenario Development***)***

Think of a vulnerability as the “Avenue of Approach” to sabotage, damage, misuse or steal an asset. As an example, you could have the strongest door, hardened hinge pins, and a sophisticated locking system to protect the asset, but there is a window (avenue of approach) in the door. The avenue of approach is through the window. The asset is not properly protected until the window is addressed. Address the vulnerability to understand if there are any mitigating circumstances associated with the window.

The process should address security weaknesses by pairing assets with threats to identify vulnerabilities that could be exploited by an adversary. General areas of vulnerability might include:

Building structure;
Equipment properties;
Operational practices;
Personnel practices;
Personal behavior; and
Locations of people, equipment and buildings;

The vulnerability levels include high, medium, and low. These levels are based on an understanding of the threat environment.

Risk Based Methodology for Physical Security Assessments

PLANNING ASSUMPTIONS CONTINUED

- Three levels of overall vulnerability identified for the facility

Level	Vulnerability description
High	No meaningful physical security measures present (beyond typical locks on doors)
Medium	Some physical security measures; but not adequate to protect against all threats identified in this report
Low	Adequate physical security measures, but could be improved

- Probability of threat is measured by past criminal activities, projected activities (identified through intelligence sources) and the environment in the community

Threat Probability	Threat level description
A. Likely	75% chance that an event will occur before and/or during the calendar year
B. Possible	10-74% chance that an event will occur sometime within the calendar year
C. Remote	At least a 1-9% chance an event will occur before the end of calendar year
D. Improbable	Less than 1% chance an undesired event will occur before the end of calendar year

Table 1

Risk Based Methodology for Physical Security Assessments

PLANNING ASSUMPTIONS CONTINUED

- Consequences of undesired event (Bombings, Arson, Demonstration, kidnapping, destruction, harassment, larceny, assault, etc.)

Event	Event Consequence
I. Catastrophic	Death, mission shutdown, severe environmental damage to facility
II. Critical	Severe Injury, partial mission shutdown, some damage to facility environment
III. Marginal	Minor injury, mission time extended, facility affected
IV. Negligible	Less than minor injury, not affecting mission, minor facility damage

RISK ASSESSMENT MATRIX

Threat Probability	I. Catastrophic	II. Critical	III. Marginal	IV. Negligible
A. Likely	I A	II A	III A	IV A
B. Possible	I B	II B	III B	IV B
C. Remote	I C	II C	III C	IV C
D. Improbable	I D	II D	III D	IV D

IA, IIA, IIIA, IB, IIB -	Unacceptable (reduce risks through countermeasures)
IVA, IIIB, IVB, IC -	Undesirable (Management decision required)
IIC, IIIC, ID -	Acceptable with review by management
IVC, IID, IIID, IVD -	Acceptable without review

Table 2

Risk Based Methodology for Physical Security Assessments

As part of the analysis of vulnerability (scenario development), existing and future (planned) security procedures and physical security equipment to protect the asset(s) must also be evaluated. A critical eye should be used to review the procedures and physical security equipment. Questions to ask and things to look for include:

- What type of protection do the procedures and/or equipment provide and what do they safeguard against?
- When and where are the procedures and/or equipment effective? Have they enhanced effectiveness?
- Have the procedures and/or equipment prevented program/project problems?
- Have the procedures and/or equipment been defeated during actual incidents or through the commissioning process?
- Is there a history of flawed procedures and/or maintenance issues with the equipment?
- Is the equipment obsolete or improperly installed?

With these answers, you are prepared to develop final, refined scenarios. This is a crucial part of the "Gap" analysis.

Risk Based Methodology for Physical Security Assessments

Step 6 - Risk Calculation/Assess Risk

Completing the remaining elements includes cause-effect analysis and an initial estimation of risk (using the risk matrix and the probability/severity table).

To establish an understanding of risk, "what if" scenarios must be assessed in terms of severity of consequences and probability of occurrence. These are subjective calculations based on limited quantitative data and judgment of knowledgeable team members. In order to calculate probability, you must decide on a definable end date (e.g., calendar year), on which to base the analysis.

Risk is the product of scenario probability/severity. The risk matrix (Table 2 lists four levels of risk and mandates specific management actions. The acceptable level of risk for an asset may vary with time, circumstances, and management's attitude toward risk. It is the owner of the asset who must ultimately decide what constitutes an acceptable level of risk for their asset. We do not want to spend thousands of dollars to protect a ten dollar asset that has low threat probabilities.

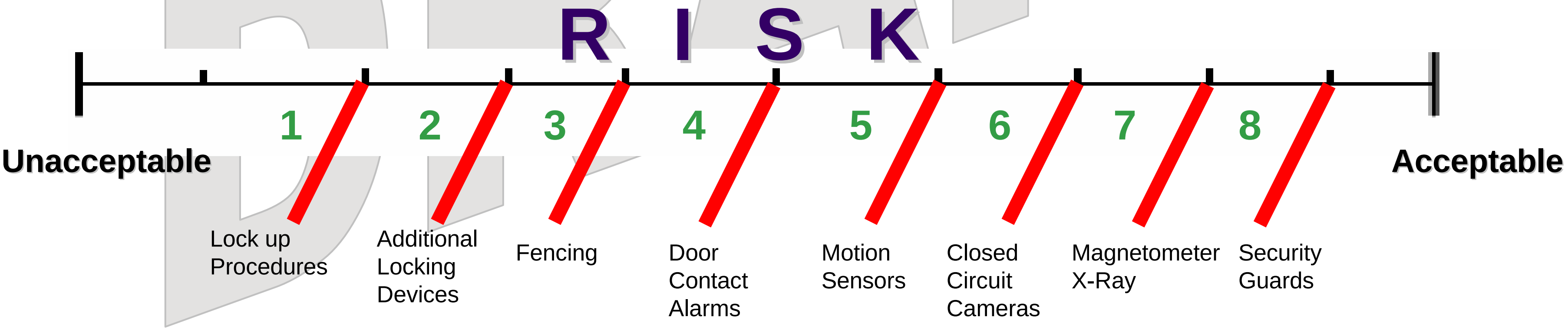
In our opening sample scenario, the team may calculate: IIC severity probability, which states acceptable with review by management.

Risk Based Methodology for Physical Security Assessments

Step 6 - Risk Calculation/Assess Risk…continued

It is impossible to eliminate all risks. All risks, in the assessment phases are determined, by default, to be unacceptable. Only when you address, analyze, and recommend security countermeasures will the risk become acceptable. This acceptance of risk is a cooperative process between the owner of the asset and the assessment team. Therefore you must be open and considerate of each persons needs and wishes based on good security practices.

As an example: On a continuum with one side stating unacceptable risks and the opposite side stating acceptable risk, we attempt through cost effective countermeasure recommendations to move from unacceptable to acceptable. You may only get to recommendation 4 when it is decided the risk has become acceptable.



Security Countermeasure Recommendations

Risk Based Methodology for Physical Security Assessments

Step 7 - Countermeasure Identification/Risk Recalculation)

Countermeasures, or corrective actions, mitigate causes and effects of scenarios. Some scenarios may simply represent reasonable interpretations. In both cases, effectiveness must be addressed (do they impact probability/severity ?).

Risk must then be recalculated considering the effectiveness of recommendations. Initial severity calculations should not change in the risk recalculation phase unless the scenario is significantly redesigned.

It should also be noted that where risks have been accepted, it is very important to include **contingency planning** as part of the risk evaluation process.

The process should rank, prioritize, and estimate importance and costs of recommendations using cost analysis technique. always starting out with recommending procedures (less costly) and then move on to technology (more costly) if needed.

After preparation and approval of the Final Draft Risk Assessment report, the countermeasure recommendations should be formatted into a Monitoring and Follow-up Tracking System.

Risk Based Methodology for Physical Security Assessments

Step 8 – Mitigation (Audit of Implemented Countermeasures)

This step involves reviews to determine if implemented recommendations have had their desired effect and have not created new, unforeseen, vulnerabilities. Each countermeasure installed should be commissioned to ensure its effectiveness.

Security Countermeasure Commissioning

1. Implement (technology and/or procedures)
2. Train personnel to perform (train the trainer)
3. Test (attempt to circumvent the countermeasure to test its reliability)
4. After action report (document the results of the test with all failures/successes)
5. Make corrections/adjustments
6. Commission (fully functional…contractor receives money)
7. Follow up (ensure the countermeasure continues to function properly)
8. Maintenance Support
9. Technical Support

<u>Important note</u>: If you do not have agreement (buy in) from the site on the implemented countermeasure, assume it will not be used effectively. If the site did not have full discussion concerning the proposed countermeasure, and they deem it not effective or useful, then the countermeasure will more than likely not be used effectively or at all. Ensure you have some level of agreement on recommendations. This is not to say you must agree with the site's disagreement, but must be able to make a common sense argument why the recommendation was made. Be prepared to defend your recommendation.