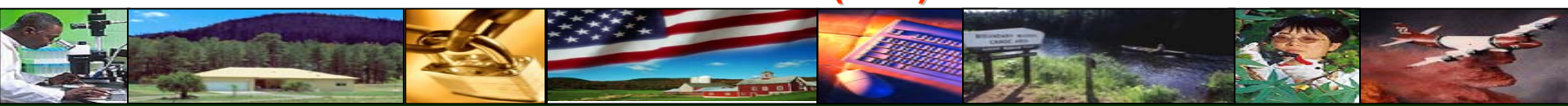
USDA Risk Management Approach

Office of Procurement and Property Management (OPPM)
Richard C. Holman (202) 720-3901



USDA Risk Management Approach

INTRODUCTION

Risk management is the technical procedure for identifying and evaluating security threats and vulnerabilities and then for balancing risks against the type (procedures/technology) and cost of security countermeasures.

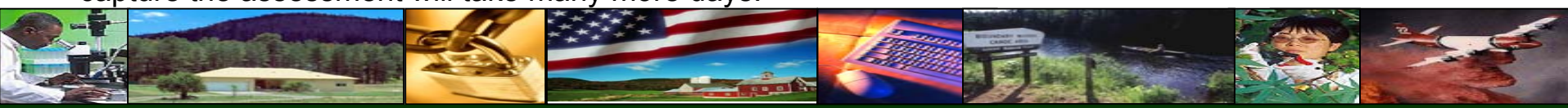
The USDA risk management methodology consists of distinct phases:

• An assessment phase which includes identifying the assets and their criticality, the degree of specific threats, vulnerability identification, and mitigation recommendations.

• A risk evaluation phase which estimates the possible impact when the critical asset is compromised, which is based on the severity and likelihood of harmful events, and consideration of controls or countermeasures.

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. See tables one and two for definitions. This is a valuable tool for managers to use in making security decisions.

Because of the flexibility of this approach, this approach can be applied to virtually any USDA facility. Depending on project scope, an assessment could take up to 2-3 days for data reviews, structured interviews and for risk evaluation, calculations, and an out briefing. The report that will capture the assessment will take many more days.



USDA Risk Management Approach

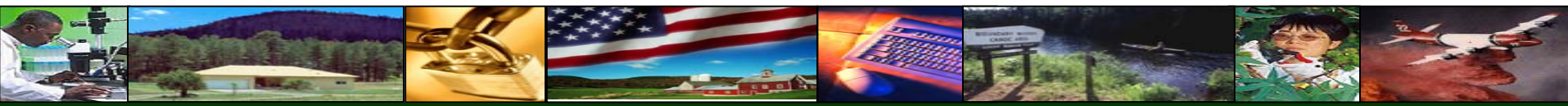
One potential limitation of this approach is the heavy reliance on team knowledge, creativity, work ethic, cooperation, and experience. Careful team selection is key to the success of risk assessments.

Each Subject Matter Expert (SME) should be cross trained to a limited degree in the other SME disciplines. This is to say, the Chemical/Biological/Radiological (CBR) SME should have some knowledge of Physical Security. This limited knowledge should be enough to identify possible vulnerabilities and then pass on those observations to the Physical Security SME for further analysis.

TEAM COMPOSITION AND TRAINING

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. For each assessment, an owner must be designated to manage both pre- and post-assessment activities.

A team leader should be appointed from outside the facility, site, project or area being assessed. Other members should be selected by understanding the site's mission and key assets. As an example, for scientific laboratories, the CBR SME should be a key member identified to assist in the assessment. As this team arrives at the site, on-site personnel with like expertise will be teamed up and work jointly with the team. The methodology requires a minimum of five team members (team size should not exceed eight).



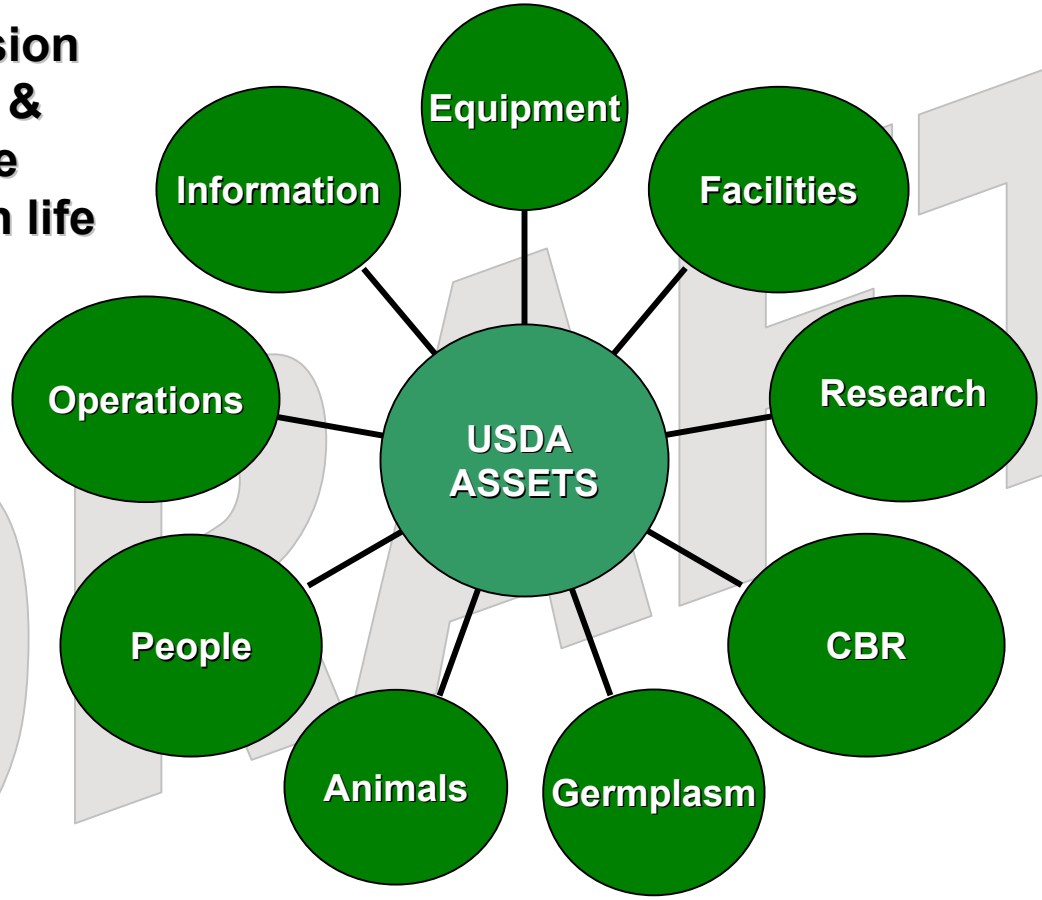
USDA Risk Management Approach

The Process very dynamic depending on World and local events.

The Risk Assessment Process – Figure 1

USDA Risk Management Approach

Essential to mission accomplishment & possible negative impact on human life and economy.



Asset Identification – Figure 2

USDA Risk Management Approach

THE QUALITATIVE RISK ASSESSMENT PROCESS

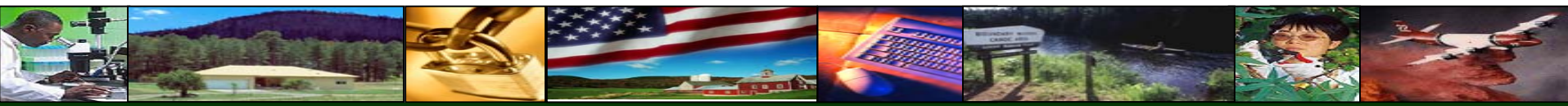
The Risk Assessment Process is comprised of eight steps which make up the assessment and evaluation phases.

Step 1 - Management Approval, Planning, and Preparation

Management, responsible for the operations being assessed, normally approves risk assessments. That approval should initiate formal planning and crafting of an execution plan. The execution plan identifies team members, scope of work, relevant information, data requirements, key interviewees (generally mid-level managers), schedule, logistics and costs. The execution plan is usually drafted by USDA/DA/OPPM. This includes a carefully constructed Statement of Work. It is important to have OPPM solicit input from management to the final plan. When finalized and distributed, the team is prepared to begin the core steps in the risk assessment process.

Step 2 - Identification of Critical Assets Requiring Protection

In this approach, critical assets (golden nuggets) and mission essential vulnerable areas (MEVAs) that are associated with critical assets (gold dust) must be identified and assessed as to their importance and weaknesses as it relates to a negative impact on the mission, environment, and populated areas. This would include such things as people, activities/operations, pathogens, chemicals, radiologicals, biologicals, information, facilities, research, and equipment. This identification of assets is done through interviews with asset owners and managers, using a structured questionnaire, data reviews, and a variety of other sources. Asset owners are generally the most knowledgeable about the assets in need of protection.



USDA Risk Management Approach

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. An example of this could be multiple offices, personnel, laboratories, etc. scattered throughout a University campus. It would be near impossible to attempt to look at each and every location and conduct an assessment in such an open environment. 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. Once assets are identified, their loss impact should be ranked from catastrophic to negligible.

USDA Risk Management Approach

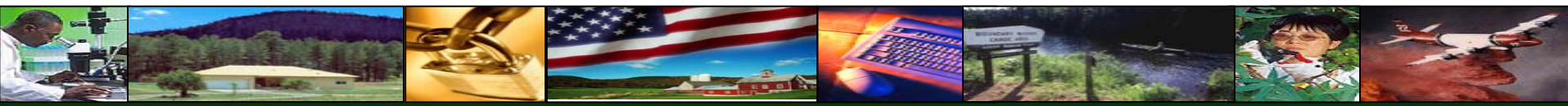
Step 3 - Threats Analysis

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, threat should he evaluated in terms of insider (our hardest to defend threat), outsider, and system induced (that is, organizational or operational flaws).

Threat, similar to assets, should he ranked in terms of likely, possible, remote, and improbable. See table one for definitions. To arrive at this, the team should 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. Are there other means of achieving these goals? Easier means: Which means will the threat choose, probability-wise?
3. What events might provoke a threat? What is the capability of the adversary? To what degree is the adversary motivated?
4. 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.



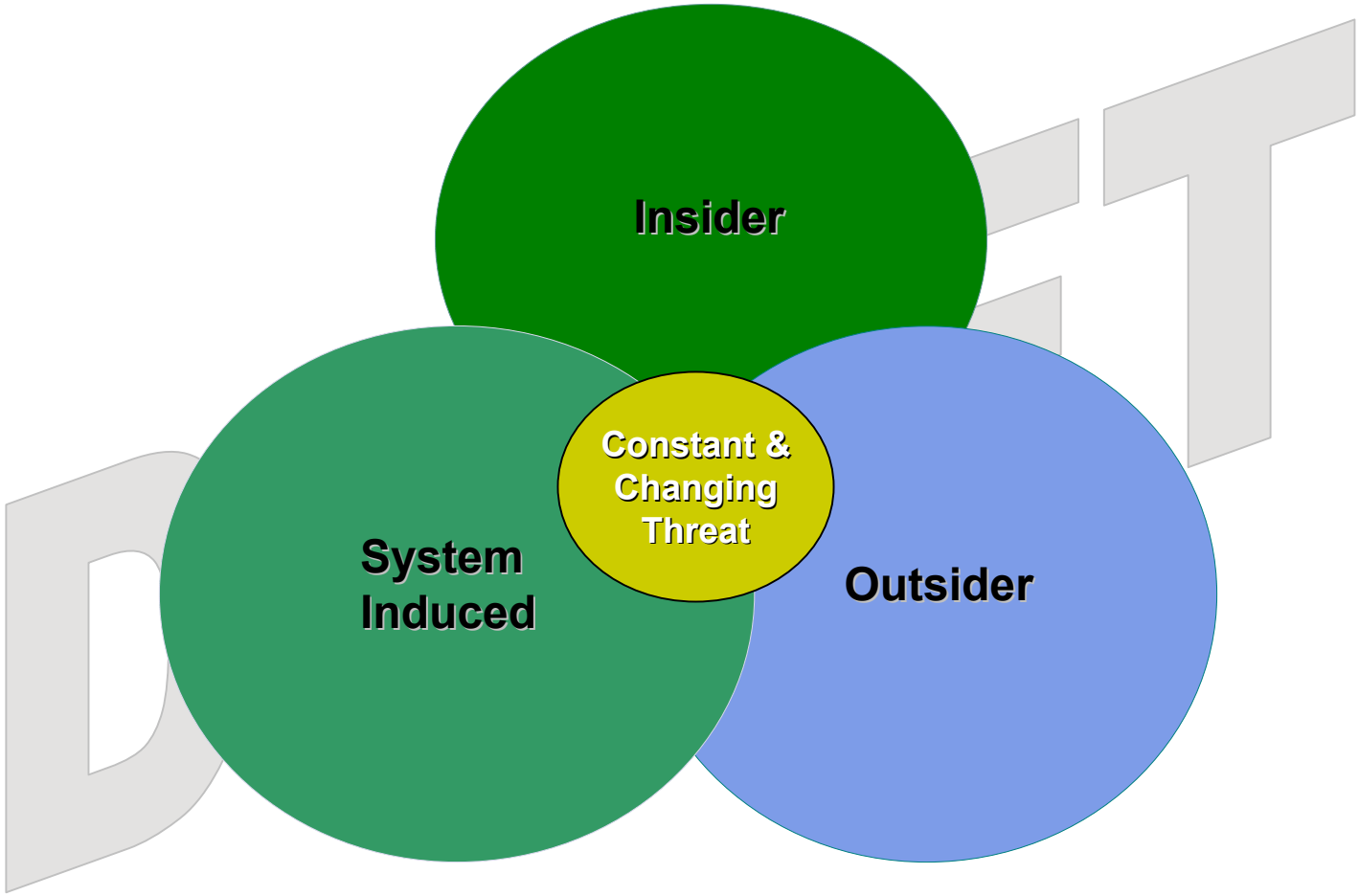
USDA Risk Management Approach

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

Types of Threat:

1. Indigenous – A specific threat to USDA assets (groups opposed to animal research, genetically modified organisms, roadless issue, etc.)
2. Domestic – Groups opposed to government intervention (Timothy McVeigh – Oklahoma bombing, Militia's, etc).
3. International – Religious fanatics that would attempt to compromise such things as USDA chemical wastes to contaminate water supplies, steal Forest Service 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 – Usually young adults creating a criminal environment due to boredom and easy access to USDA assets.
6. Disgruntled Employee – Someone that is not happy with a specific office and will use internal measures to perpetrate a crime to the USDA asset.
7. System Induced – No emergency backup power for a sub-zero freezer containing sensitive DNA material.

USDA Risk Management Approach



Identification of Threat – Figure 3

USDA Risk Management Approach

Step 4 – Gap Analysis

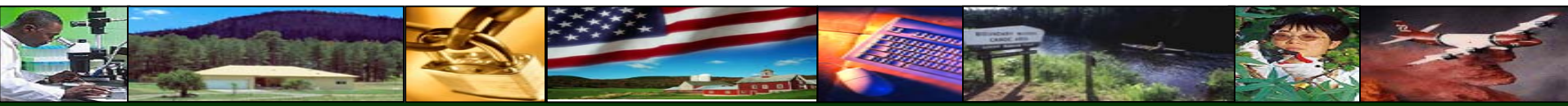
The “Gap” is the difference between the present asset protection level and the protection level required after a risk and threat analyses have been completed.

1. Once the asset and its characteristics have been identified, and the type of threat 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.



USDA Risk Management Approach

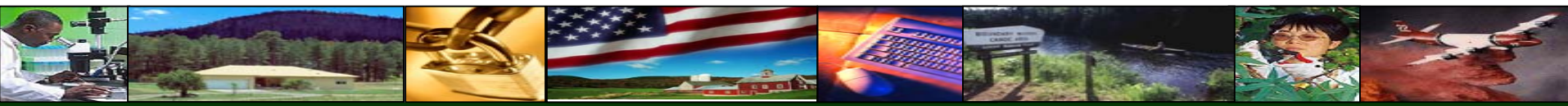
Step 5 - Analysis of Vulnerability (Scenario Development*)*

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

Building characteristics:
Equipment properties:
Operational practices:
Personnel practices;
Personal behavior;
Locations of people, equipment and buildings; and
Nature of operations.

Think of a vulnerability as the “Avenue of Approach” to the 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 vulnerability levels include high, medium, and low. These levels are based on the team’s understanding of the threat environment. See table one for definitions.



USDA Risk Management Approach

PLANNING ASSUMTIONS CONTINUED

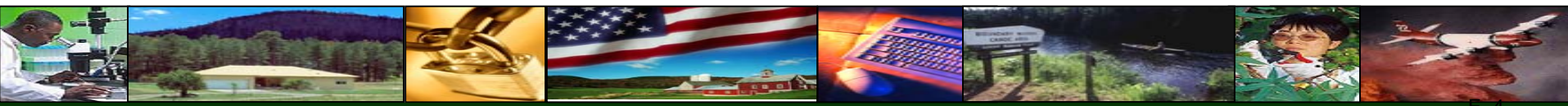
- Three levels of overall vulnerability identified for the facility

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



USDA Risk Management Approach

PLANNING ASSUMTIONS 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

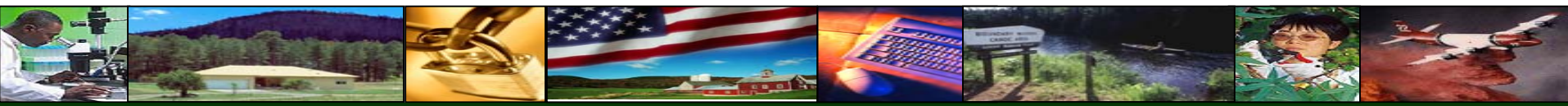
USDA Risk Management Approach

Consideration of existing and future (planed) security countermeasures must also be evaluated. Questions to ask and things to look for include:

- What type of protection do they provide and what do they safeguard against?
- When and where are they effective? Have they enhanced effectiveness?
- Have they prevented program/project problems?
- Have they been defeated during actual incidents or through the commissioning process?
- What is their history of flawed operations or maintenance issues?
- Obsolete or faulty equipment?
- Poor training by end user:
- Human error; and
- Poor maintenance of equipment.

With these answers, the team is prepared to develop final, refined scenarios. This is a crucial part of the “Gap” analysis, but should not only be used for that purpose. A critical eye should be used to look at these countermeasures.

There may be a great intrusion detection system in a facility, but because of the many false alarms, the system was turned off without exploring the reasons for the high rate of false alarms. As an example, a motion detector could annunciate each time the HVAC comes on and moves an open flap of a box. The simple fix is to develop a procedure for all storage boxes to be completely closed, and therefore no more false alarms, then one can turn the system back on.



USDA Risk Management Approach

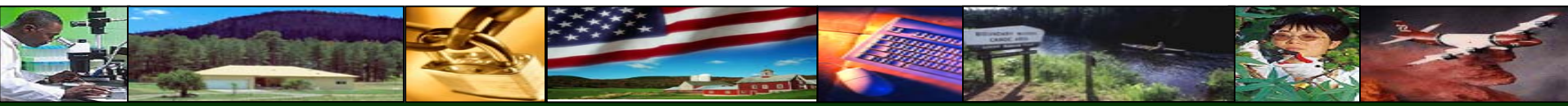
Step 6 - Risk Calculation/Assess Risk

The team will now complete the remaining elements including causes-effect analysis and an initial estimation of risk (using the risk matrix and the probability/severity table). Reference tables one and two.

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, teams must decide on a definable end date (e.g., calendar year), 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 first sample scenario, the team may calculate: IIC severity probability, which states acceptable with review by management.

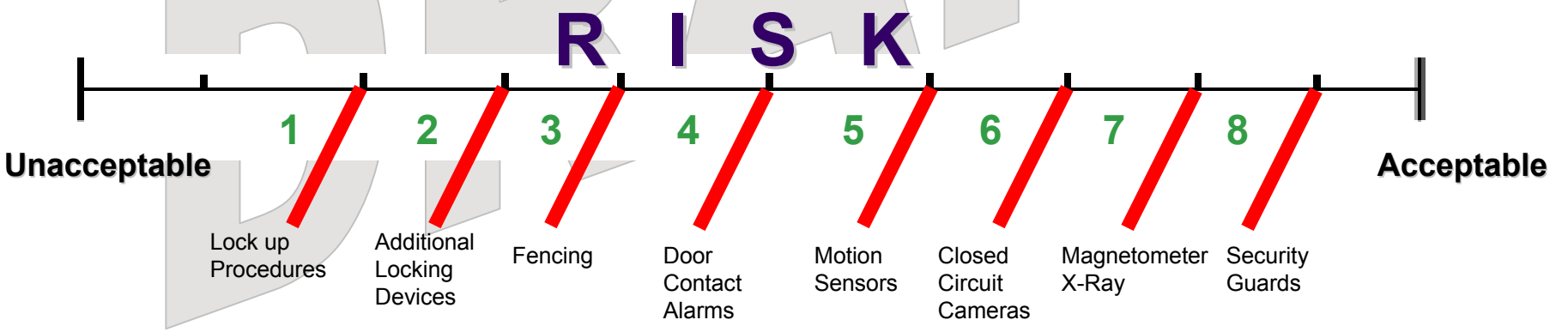


USDA Risk Management Approach

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

USDA Risk Management Approach

Step 7 - Countermeasure Identification/Risk Recalculation)

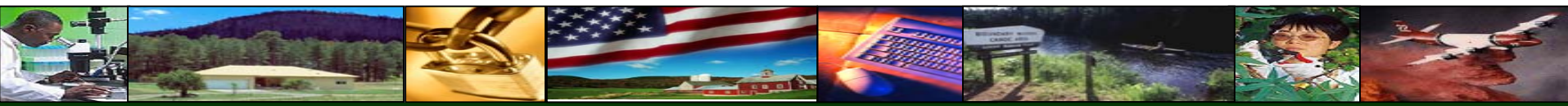
Countermeasures, or corrective actions, mitigate causes and effects of scenarios. Some scenarios may simply represent reasonable interpretations by the team. In both cases, effectiveness must be addressed (do they impact probability/severity).

The team must then recalculate risk 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 team must also rank, prioritize, and estimate importance and costs of recommendations using cost analysis technique. Always start 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.



USDA Risk Management Approach

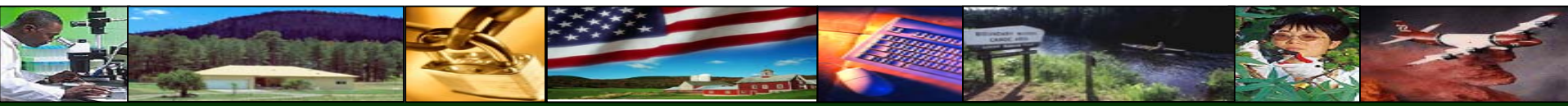
Step 8 – Mitigation (Audit of Implemented Countermeasures)

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

Important note: If you do not have agreement (buy in) from the site on the implemented countermeasure, assume it will not be used effectively. This is to say, 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.



USDA Risk Management Approach

Wrap Up:

1. Ensure you properly identify the asset through a detailed discussion with the site and then have the expertise to properly evaluate the security of the asset and it's many potential harmful impacts.

2. Look at all forms of threats from all sources of information (Local police, FBI, State Homeland Security, Unions, etc.). Use your imagination.

3. Understand the dynamics of the asset and when it is most vulnerable to an attack.

4. Make common sense security countermeasure recommendations and get buy in from the site. Don't build a fortress environment that people must work in every day.

5. Ensure the security countermeasures are affective by testing and retesting. The changing of the threat could make the countermeasure ineffective over a period of time.

6. Provide communication links to the site for any future follow up questions or proposed actions.