

## **RISK MANAGEMENT**

D. T. Coulter

Risk management is the application of money and manpower to achieve a cost-effective investment in countermeasures within an organization. Effective risk management minimizes both risk and costs. Risk management is a systematic and analytical process to consider the probability that a threat will endanger an asset, individual, or function and to identify countermeasures to minimize the risk and mitigate the consequences of an attack. Risk management principles accept that while risk cannot be eliminated; improving protection from known or potential threats can reduce it. It is generally accepted that risk is a function of threat, vulnerability and consequence. Once assets, personnel and critical functions have been identified and prioritized, a proven risk management approach includes three primary elements: identifying and evaluating credible threats, identifying and assessing vulnerabilities and evaluating consequences if the assets are compromised or destroyed. If any of the three elements are zero, there is no risk. Risk is defined as the possibility of loss or injury. To be a risk, therefore, an event must:

- Be in the future
- Be uncertain
- Result in a loss or a consequence to the program should an event occur.

Events that do not fit these criteria are not risks. In particular, an event that has already occurred is not a risk, an event that is certain to occur is not a risk, and an event whose consequence is neither a gain nor a loss is not a risk.

One challenge is that many people classify several issues as risks that are, in fact, problems...events that have already occurred that result in costly consequences. Whereas risks can be mitigated, problems must be solved. It is certainly possible that the future consequences of a problem may not be fully known; in that case, the unknown consequences are properly classified as risks and, as such, may be candidates for mitigation or contingency plans. However, people must be able to distinguish between the program activities of solving a problem, something that must be done, and mitigating a risk, something that is optional.

As there is little agreement among industry experts on defining risk management. For purposes of this monograph, the following activities will comprise risk management: Risk Assessment, Risk Identification, Risk Mitigation, and Risk Monitoring. Note that these activities form a cycle and that as programs progress there may be several iterations of assessment, identification, mitigation, and monitoring.

Risk identification consists of determining what uncertain future events are possible. In the identification activity, care should be taken to ensure that the items identified are truly risks, as opposed to problems or to future events that are certain; management must be certain that the list of risks is not too long. Simultaneously, historical problems should be

researched and team members' imaginations exercised to ensure that potential risks are not overlooked; management must be certain that the list is not too short, as well.

Once risks are identified, they must be analyzed to determine the likelihood of occurrence, and the range of possible consequences. This is another area in which historical data can be useful to help assess probabilities and potential costs. Risk assessment is also the activity in which management establishes the thresholds for risk mitigation and contingency planning: what level of risk is acceptable and what level requires additional investment.

Risk mitigation is the activity in which countermeasures and contingency plans are formulated and put into practice. Put another way, risk mitigation is the activity in which the cost of insurance occurs.

Risk monitoring comprises a number of tasks. If risk events occur, risk monitoring is the activity that assesses the effectiveness of the risk mitigation strategies and contingency plans. Risk monitoring is the activity that determines when overall risk is reduced because of the implementation of risk management plans or because risk events have not occurred. Risk monitoring is the activity that produces reports and evaluations on the overall risk of the program.

Too often, management views risk management as no more than an item to be checked off on a form: *"I did my risk management, now I can get back to doing real work."* To be effective, risk management requires the same level of dedication as every other task in a successful program. Management must understand and promote the importance of risk management as an essential component of the program, and must actively support risk management activities by team members. With proper backing from management, risk management activities will then be viewed as "real work".

Several difficulties in risk management may occur regularly. Management is encouraged to study this list, to evaluate their teams in these areas, and to develop methods to correct shortcomings where they are identified:

- Difficulty distinguishing risks from problems.
- Difficulty distinguishing normal business practices from risk mitigation and contingency planning.
- Difficulty distinguishing between certain future events and uncertain future events.
- Difficulty envisioning potential future (risk) events.
- Reluctance to mitigate risks.
- Excessive optimism.
- Lack of systematic risk identification, risk assessment, risk mitigation, and risk monitoring procedures.
- The view that risk management activities take time away from doing "real work"

For risk management to be effective it must permeate at every level within the program. The risks facing a program or facility must be fully understood and mitigated when appropriate. The remaining risk should be closely monitored and managed accordingly with well vetted contingency plans. When implemented properly, risk management can provide the difference between successful programs and those that fail.