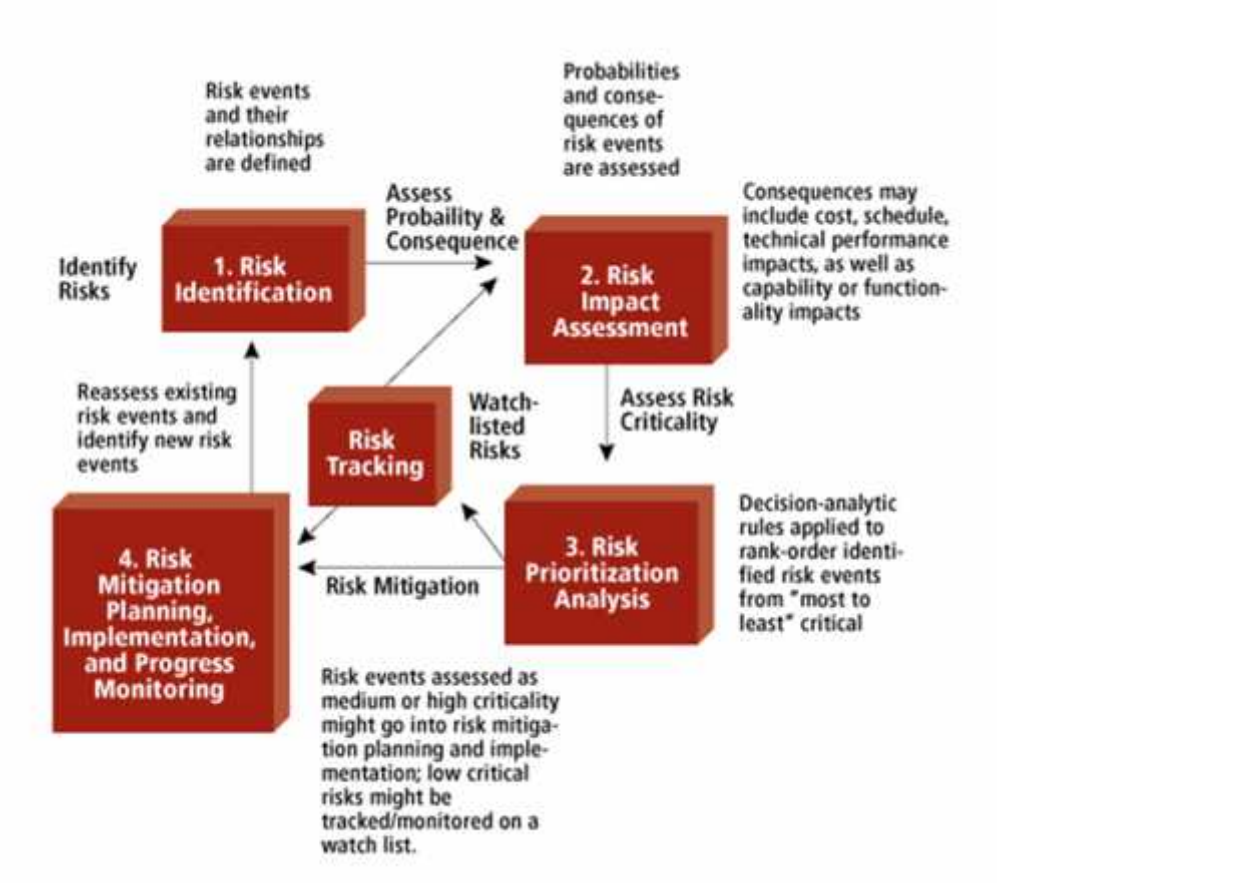
MODULE 12 MITIGATION OF BUSINESS CRITICAL RISK AREAS

Introduction –

1. Risk mitigation planning is the process of developing options and actions to enhance opportunities and reduce threats to project objectives.
2. Risk mitigation implementation is the process of executing risk mitigation actions.
3. Risk mitigation progress monitoring includes tracking identified risks, identifying new risks, and evaluating risk process effectiveness throughout the project.

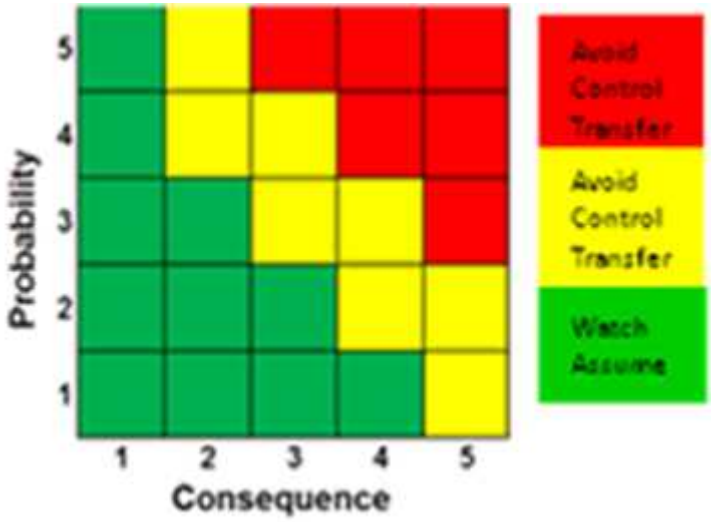
Risk mitigation planning, implementation, and progress monitoring are depicted in the below diagram. As a part of an iterative process, the risk tracking tool is used to record the results of risk prioritization analysis (step 3) that provides input to both risk mitigation (step 4) and risk impact assessment (step 2).



The risk mitigation step involves development of mitigation plans designed to manage, eliminate, or reduce risk to an acceptable level. Once a plan is implemented, it is continually monitored to assess its efficacy with the intent of revising the course-of-action if needed.

Risk Mitigation Strategies –

General guidelines for applying risk mitigation handling options are shown in Figure 2. These options are based on the assessed combination of the probability of occurrence and severity of the consequence for an identified risk. These guidelines are appropriate for many, but not all, projects and programs.



Risk mitigation handling options include:

- Assume/Accept: Acknowledge the existence of a particular risk, and make a deliberate decision to accept it without engaging in special efforts to control it. Approval of project or program leaders is required.
- Avoid: Adjust program requirements or constraints to eliminate or reduce the risk. This adjustment could be accommodated by a change in funding, schedule, or technical requirements.
- Control: Implement actions to minimize the impact or likelihood of the risk.
- Transfer: Reassign organizational accountability, responsibility, and authority to another stakeholder willing to accept the risk.
- Watch/Monitor: Monitor the environment for changes that affect the nature and/or the impact of the risk.

Each of these options requires developing a plan that is implemented and monitored for effectiveness.

From a systems engineering perspective, common methods of risk reduction or mitigation with identified program risks include the following, listed in order of increasing seriousness of the risk

1. Intensified technical and management reviews of the engineering process
2. Special oversight of designated component engineering
3. Special analysis and testing of critical design items
4. Rapid prototyping and test feedback
5. Consideration of relieving critical design requirements
6. Initiation of fallback parallel developments

When determining the method for risk mitigation, security risk assessment can help their customers to assess the performance, schedule and cost impacts of one mitigation strategy over another. For something like "parallel" development mitigation.

Best Practices –

1. Handling Options
   - Assume/Accept. Collaborate with the operational users to create a collective understanding of risks and their implications. Risks can be characterized as impacting traditional cost, schedule, and performance parameters. Risks should also be characterized as impact to mission performance resulting from reduced technical performance or capability. Develop an understanding of all these impacts. Bringing users into the mission impact characterization is particularly important to selecting which "assume/accept" option is ultimately chosen. Users will decide whether accepting the consequences of a risk is acceptable. Provide the users with the vulnerabilities affecting a risk, countermeasures that can be performed, and residual risk that may occur. Help the users understand the costs in terms of time and money.
   - Avoid. Again, work with users to achieve a collective understanding of the implications of risks. Provide users with projections of schedule adjustments needed to reduce risk associated with technology maturity or additional development to improve performance. Identify capabilities that will be delayed and any impacts resulting from dependencies on other efforts. This information better enables users to interpret the operational implications of an "avoid" option.
   - Control. Help control risks by performing analyses of various mitigation options. For example, one option is to use a commercially available capability instead of a contractor developed one. In developing options for controlling risk in your program, seek out potential solutions from similar risk situations of other organizations customers industry, and academia. When considering a solution from another organization, take special care in assessing any architectural changes needed and their implications.
   - Transfer. Reassigning accountability, responsibility, or authority for a risk area to another organization can be a double-edged sword. It may make sense when the risk involves a narrow specialized area of expertise not normally found in program offices. But,

transferring a risk to another organization can result in dependencies and loss of control that may have their own complications. Position yourself and your customer to consider a transfer option by acquiring and maintaining awareness of organizations within your customer space that focus on specialized needs and their solutions. Acquire this awareness as early in the program acquisition cycle as possible, when transfer options are more easily implemented.

- Watch/Monitor. Once a risk has been identified and a plan put in place to manage it, there can be a tendency to adopt a "heads down" attitude, particularly if the execution of the mitigation appears to be operating on "cruise control." Resist that inclination. Periodically revisit the basic assumptions and premises of the risk. Scan the environment to see whether the situation has changed in a way that affects the nature or impact of the risk. The risk may have changed sufficiently so that the current mitigation is ineffective and needs to be scrapped in favor of a different one. On the other hand, the risk may have diminished in a way that allows resources devoted to it to be redirected.

2. Determining Mitigation Plans
   - Understand the users and their needs. The users/operational decision makers will be the decision authority for accepting and avoiding risks. Maintain a close relationship with the user community throughout the system engineering life cycle. Realize that mission accomplishment is paramount to the user community and acceptance of residual risk should be firmly rooted in a mission decision.
   - Seek out the experts and use them. Seek out the experts within and outside MITRE. MITRE's technical centers exist to provide support in their specialty areas. They understand what's feasible, what's worked and been implemented, what's easy, and what's hard. They have the knowledge and experience essential to risk assessment in their area of expertise. Know our internal centers of excellence, cultivate relationships with them, and know when and how to use them.
   - Seek out the experts and use them. Seek out the experts within and outside of your organization to provide support in their specialty areas. They understand what's feasible, what's worked and been implemented, what's easy, and what's hard. They have the knowledge and experience essential to risk assessment in their area of expertise. Know our internal centers of excellence, cultivate relationships with them, and know when and how to use them.
   - Recognize risks that recur. Identify and maintain awareness of the risks that are "always there" interfaces, dependencies, changes in needs, environment and requirements, information security, and gaps or holes in contractor and program office skill sets. Help create an acceptance by the government that these risks will occur and recur and that plans for mitigation are needed up front. Recommend various mitigation approaches including adoption of an evolution strategy, prototyping, experimentation, engagement with broader stakeholder community, and the like.

- Encourage risk taking. Given all that has been said in this article and its companions, this may appear to be an odd piece of advice. The point is that there are consequences of not taking risks, some of which may be negative. Help the customer and users understand that reality and the potential consequences of being overly timid and not taking certain risks in your program. An example of a negative consequence for not taking a risk when delivering a full capability is that an adversary might realize a gain against our operational users. Risks are not defeats, but simply bumps in the road that need to be anticipated and dealt with.
- Recognize opportunities. Help the government understand and see opportunities that may arise from a risk. When considering alternatives for managing a particular risk, be sure to assess whether they provide an opportunistic advantage by improving performance, capacity, flexibility, or desirable attributes in other areas not directly associated with the risk.
- Encourage deliberate consideration of mitigation options. This piece of advice is good anytime, but particularly when supporting a fast-paced, quick reaction government program that is juggling many competing priorities. Carefully analyze mitigation options and encourage thorough discussion by the program team. This is the form of the wisdom "go slow to go fast."
- Not all risks require mitigation plans. Risk events assessed as medium or high criticality should go into risk mitigation planning and implementation. On the other hand, consider whether some low criticality risks might just be tracked and monitored on a watch list. Husband your risk-related resources.

3. What actions are needed?
    - Make sure you have the right exit criteria for each. For example, appropriate decisions, agreements, and actions resulting from a meeting would be required for exit, not merely the fact that the meeting was held.
    - Look for evaluation, proof, and validation of met criteria. Consider, for example, metrics or test events.
    - Include only and all stakeholders relevant to the step, action, or decisions.

4. When must actions be completed?
    - Backward Planning: Evaluate the risk impact and schedule of need for the successful completion of the program and evaluate test events, design considerations, and more.
    - Forward Planning: Determine the time needed to complete each action step and when the expected completion date should be.
    - Evaluate key decision points and determine when a move to a contingency plan should be taken.
5. Who is the responsible action owner?
6. What resources are required? Consider, for example, additional funding or collaboration.
7. How will this action reduce the probability or severity of impact?

8. Develop a contingency plan ("fall back, plan B") for any high risk.
    - Are cues and triggers identified to activate contingency plans and risk reviews?
    - Include decision point dates to move to fallback plans. The date to move must allow time to execute the contingency plan.
9. Evaluate the status of each action.
    - Determine when each action is expected to be completed successfully.
10. Integrate plans into IMS and program management baselines.
    Risk plans are integral to the program, not something apart from it.
11. Monitoring Risk
    - Include risk monitoring as part of the program review and manage continuously. Monitoring risks should be a standard part of program reviews. At the same time, risks should be managed continuously rather than just before a program review. Routinely review plans in management meetings.
    - Review and track risk mitigation actions for progress. Determine when each action is expected to be completed successfully.
    - Refine and redefine strategies and action steps as needed.
    - Revisit risk analysis as plans and actions are successfully completed. Are the risks burning down? Evaluate impact to program critical path.
    - Routinely reassess the program's risk exposure. Evaluate the current environment for new risks or modification to existing risks.