Lesson 7
Risk Management
Overall: Given a DoD IT/SW acquisition scenario, apply DoD Risk Management (RM) policy in support of the program’s objectives and priorities.

- Define the elements that constitute an effective RM program for an Information Technology (IT) system acquisition.
- Identify the two components of risk.
- Identify how risk, issue, and opportunity management interrelate.
- Identify risks inherent to IT system acquisition.
- Apply the five components of the DOD RM Process Model to a given IT acquisition scenario.
Lesson Overview

Overview

- Risk, Issue, and Opportunity Relationship
- IT Related Risks
- Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
- Lesson Review

“If you don’t actively attack the risks, they will actively attack you.”

Tom Gilb

Principles of Software Engineering Management
DoD Risk, Issue, and Opportunity Guide, Jan 2017

- The PM is responsible for implementing effective risk management within program constraints.
- Successful risk management requires planning and resourcing, and should be implemented early in the life cycle beginning with the Materiel Solution Analysis (MSA) phase or earlier.

DoD RIOM Guide Content

- Section 1: Introduces the scope and overview of the guide.
- Section 2: Describes how risk informs the decisions shaping a program acquisition strategy and structure, and the most important activities to manage risk by life cycle phase.
- Section 3: Describes how a program manages risks and issues by developing plans to reduce the consequences and/or the likelihood of the risks or issues.
- Section 4: Describes opportunity management, including the similarities and differences between opportunity and risk management.
- Section 5: Highlights considerations to manage risks related to internal and external interfaces with interdependent programs. Discusses the different priorities of interdependent programs and techniques to manage and mitigate cross-program risks.
Risk, Issue, and Opportunity Definitions

• **Risks** are potential future events or conditions that may have a negative effect on achieving program objectives for cost, schedule, and performance. Risks are defined by (1) the probability (greater than 0, less than 1) of an undesired event or condition and (2) the consequences, impact, or severity of the undesired event, were it to occur.

• **Issues** are events or conditions with negative effect that have occurred (such as realized risks) or are certain to occur (probability of 1) that should be addressed.

• **Opportunities** have potential future benefits to the program’s cost, schedule, and/or performance baseline.

Source: Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, Jan 2017
Risk Management

Risk, Issue, and Opportunity Relationship

**Technical**
- Technology
- Engineering
- Integration
- Manufacturing

**Programmatic**
- Schedule
- Staffing
- Communication
- Estimates

**Business**
- Laws
- Dependencies
- Resources
- Customer

**Consequences:**
Both positive and negative impacts to cost, schedule, and performance
Risks and Issues

Issues: **Current** Problems: Focus is on Real-Time Consequences

Risks: **Future** Problems: Focus is on Future Consequences and Likelihood

**RISK or ISSUE?**

If it has already occurred, it’s an **Issue**, not a **Risk**

**Issues** may create additional potential **Risks**
Lesson Overview

“If you don’t actively attack the risks, they will actively attack you.”
Tom Gilb

Principles of Software Engineering Management
• OSD has found that program issues are, too often, mistakenly characterized as risks.
  – This practice is reactive and tends to blind the program to true risk management. Risk management applies resources to lessen the likelihood, or in some cases, the consequence, of a future event.

• Issue management, on the other hand, applies resources to address and resolve a past or occurring event and its related consequences.
  – When a negative event has been identified and has a past or present impact to the cost, schedule, or performance of a program, it is not a risk.
  – These events should be cataloged as issues and should be addressed within the program’s normal issue management process.
  – In addition, even though an issue may introduce a likely future consequence, this does not make it a risk.
  – To ensure issues and risks are properly identified, programs should have an issue management approach to identify problems and track associated closure plans.
  – Programs should also assess whether issues are spawning prospective risks.
The key is to ensure proper focus on both issues and risks so that attention on current problems will not overtake efforts to manage risks and opportunities.

- Applies resources to address and resolve the consequences associated with a past, present, or certain future event.
- Programs also should assess whether issues may create additional potential risks, and evaluate them accordingly.
- Issue management and opportunity management are complementary to the risk management process.
Issues – Identification

• Issues are best identified before the beginning of a new project or contract and should be updated and reviewed periodically throughout the life cycle of the program.

• Unlike opportunities and risks, there is no assessment of their likelihood because issues have either already occurred or are in the process of occurring.

Source: Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, Jan 17
• Approved issues should be analyzed using the program’s risk management consequence criteria, and the results entered into an issue tracking register.

• Unlike opportunities and risks, no evaluation of issue likelihood is necessary as the probability=1.

• Using the top row from the risk matrix, the issue consequence value is then converted to an issue level using the issue reporting matrix.

• The results are entered into the program’s issue tracking register.

**Issue reporting matrix**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Consequence</th>
<th>Type</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue X (describe the issue that has occurred or will occur, the type of issue [technical, business, or programmatic], and the resulting cost, schedule, and performance consequences)</td>
<td>TECH (T)</td>
<td>[P] – 10/12/13</td>
<td>$1M</td>
</tr>
<tr>
<td>Activity 1</td>
<td>[P]</td>
<td>[A]</td>
<td>R&amp;D &amp; E</td>
</tr>
<tr>
<td>Activity 2</td>
<td>[P]</td>
<td>[A]</td>
<td>Procurement</td>
</tr>
<tr>
<td>Activity 3</td>
<td>[P]</td>
<td>[A]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Issue Tracking Register**

DoD Risk, Issue, and Opportunity Management Guide Jan 2017
The program should evaluate the options for correction in terms of cost, schedule, performance, and residual risk, and select the best option (or hybrid of options) consistent with program circumstances. The primary options for issues are:

- **Ignore**: Accept the consequences without further action based on results of a cost/schedule/performance business case analysis.

- **Control**: Implement a plan to reduce issue consequences and residual risk to as low a level as practical or minimize impact on the program.

- **Less common options include Avoid and Transfer**, which carry the same definitions for issues as they do for risks. Avoid is sometimes considered one version of Control and subsumed in that option.
• Programs should not confuse issues with risks.
• Issues are assessed for residual risks and formal risks are established as appropriate.
• Programs document an issue management process.
• The process may share elements with the risk management process, while respecting differences.
• Programs develop a plan to address, track, and review issues during regular meetings and reviews.
• Programs track cost, schedule, and performance issues and report to the appropriate management level based upon the level of the consequence impacts.
Opportunity Management

- Opportunities are potential future benefits to the program’s cost, schedule, and/or performance baseline.
- The program identifies potential enhancements to cost, schedule, and/or performance.
- Measures potential program improvement in terms of likelihood and benefits.
- Opportunities should be evaluated for both advantages and disadvantages.

Opportunity management, like issue management, should be considered as complementary to risk management.
• PMs use opportunity management to plan, identify, analyze, handle, and monitor initiatives that potentially yield improvements in the cost, schedule, and/or performance baseline.

• Programs evaluate approved opportunities and manage any associated risks.

Programs establish opportunity likelihood and benefit criteria in line with program “should-cost” objectives.
• Achieve Affordable Programs

• Control Costs Throughout the Product Lifecycle

• Incentivize Productivity & Innovation in Industry and Government

• Eliminate Unproductive Processes and Bureaucracy

• Promote Effective Competition

• Improve Tradecraft in Acquisition of Services

• Improve the Professionalism of the Total Acquisition Workforce
• All acquisition managers should **routinely analyze all cost elements** and look at reasonable measures to reduce them with prudent consideration of risks
• Don’t accept the Independent Cost Estimate (ICE) as a self-fulfilling prophesy
• The goal is **not** to spend the budget—it’s to get all the value for the budget
• Should cost targets are required for all Acquisition Category (ACAT) I–III (services and products) programs

**Note:** Should Cost is for internal DoD use, not for budget planning
• Risk Overview
• Risk, Issue, and Opportunity Relationship

• **IT Related Risks**

• Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3

• Lesson Review
Sources/Categories of Common IT Risks

- Changing and/or creeping requirements
- Government Off the Shelf (GOTS) Software development
- Pace of tech advancement
- Mature technology availability challenges
- Technical feasibility
- Interdependence of parallel projects
- Sheer # and scope of projects
- Funding availability & stability

- Commercial Off the Shelf (COTS)
- System integration
- GOTS Software Reuse (NDI)
- Architecture challenges
- Cybersecurity
- SW T&E
- Data quality challenges
- Interfaces (user, data, communications, …)
- Personnel/ Training challenges
• Risk Overview
• Risk, Issue, and Opportunity Relationship
• IT Related Risks

• Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3

• Lesson Review
Risk management is an integral part of program management and systems engineering.

Successful risk management requires thoughtful planning and resourcing, and should be implemented as early as possible in the life cycle.

Effective qualitative and quantitative risk, issue, and opportunity management are critical to a program’s success.

The goal is to identify risks and handling strategies to inform decisions before they become issues.
• Helps identify and anticipate problems
• Provides for sufficient response time
• Eliminates many surprises
• Provides pro-active approach
• Prevents loss of: revenue, time and mission success

One risk-mitigation rule of thumb for program planning is to do the hard things first.
Hon. Frank Kendall, USD/AT&L
• **Culture** often precludes risk management
  - I know what I’m doing
• **Going through the motions** vs. an Integral process
  - Time for another quarterly brief
• Management and organizations fear risk identification
  - It’s not my fault
  - If I don’t know, then no one can blame me
• **Issues vs. risks**—they are not the same
  - I just lost $2M in the budget review
• **Process is not supported by infrastructure**
  - Who is in charge of risk management?
When establishing risk processes and procedures:

• Assign roles, responsibilities, and authorities

• Select and document overall approach:
  – Process and procedures
  – Risk analysis criteria for likelihood and consequences
  – Risk mitigation procedures

• Establish traceability of risk to technical requirements and overall program objectives

• Align government and contractor roles, responsibilities, tools, and information exchange

• Determine risk management resources, to include budget, facilities, personnel, schedule

• Determine risk management battle rhythm

Source: Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, Jan 17
Details of Roles and Responsibilities contained in Appendix D of RIOMG
DoD programs are required to summarize the risk management approach and planning activities in the SEP and Acquisition Strategy. Some programs document their plans in a combined Risk, Issue, and Opportunity (RIO) Management Plan Plan or in a Risk Management Plan (RMP).

**Suggested RMP outline:**
- Introduction
- Program Summary
- Definitions
- Risk Management Strategy
- Risk Management Board(s) and Risk Working Group(s)
- Roles, Responsibilities, and Authorities
- Risk Management Process and Procedures
- Risk Management in Relation to Other PM Tools
- Risk Evaluation Techniques
- Communicating and Feedback Process
“I cannot imagine any conditions which would cause a ship to founder. I cannot conceive of any vital disaster happening to this vessel. Modern shipbuilding has gone beyond that ..."

Captain E.J. Smith, 1906, about the Adriatic
(Captain of Titanic on the evening on 14 April, 1912)
Risk Identification - What can go wrong?

When identifying risks:

- Understand the nature of the product and the requirements that shape the product.
- Use various risk ID methodologies:
  - Independent assessments
  - SOW requirements
  - Brainstorming sessions with SMEs
  - Interviews with IPT leads, Systems Command/Center competencies
  - Review of similar/historical programs
  - Trade studies
- Review analysis of Technical Performance Measures, resource data, life cycle cost information, WBS/IMS/EVM data trends, and progress against critical path.
- Assess technical performance at all levels: component, subsystem, integrated product, external interfaces. How big a gap? How challenging to cross it?
Cast your net wide at first! Do not ignore areas or eliminate ideas early in the process.

All program personnel are encouraged to identify candidate risks.
Identifying Risk Ideas: Technical Risk Drivers

- Requirements
- Proprietary Data/Designs
- Technology
- Hardware State-of-the-Art
- Support Concepts
- Reliability and Maintenance
- Constraints
- Personnel
- Computer Resources
- Manufacturing Resources
- New Manufacturing/labs
- Standards
- Government Furnished Equipment/Personnel
- Environment

- Tools
- Data Rights
- Experience
- Documentation
- Management Approach

Software Specific Risks
- Complexity
- Size
- Stability
- Developmental Approach
- Process Model
- Process Maturity
- Integration Approach
Good “If Then” Statements are Critical to effective Risk Management…

… but they are not enough. We must know WHY in order to do something about it (handling).
Ask “Why” multiple times until the root risk event(s) is (are) discovered.
Example Risk Statements

- The project is at risk of running over budget
- If a large part of the software must now be written in C++, then the time required to train the development team in C++ will extend the project’s schedule by 3 months
- If DII-COE version 1.5 is more than 1 month late, then program xyz release 1 will experience a day for day schedule slip
- If customer-facing systems fail as customer volumes increase then revenue stream to supplier will be negatively impacted
• Risk Overview
• Risk, Issue, and Opportunity Relationship
• IT Related Risks
• Risk Management Process

- Exercise 1
  - Exercise 2
  - Exercise 3

• Lesson Review
TASK: Write a proper Risk Statement for each of the following while you answer the question: “What could happen to us in Post Deployment Software Support (PDSS) Phase if things don’t change now?” Assume YOU are the PM stated in the situation.

- **Team 1**: PM JTAMS is re-using Army TAMS software. The TAMS OBD application has over 900 patches to it.
- **Team 2**: PM JTAMS is re-using Army TAMS software. All of the TAMS applications (OBD, PAMS and THS) come to us without documentation.
- **Team 3**: PM Firebird (FUAV) is using 50,000 SLOC of an old/obsolete programming language called TACPOL.
- **Team 4**: PM JTAMS is experiencing delays in the receipt of MRES software updates.
- **Team 5**: PM JCCS keeps changing their interfaces with FUAV, JUGV and JTAMS. As a result, PM JTAMS has no interface to design to.
Risk Analysis - How big is the risk?

When analyzing risks:

- Quantify the cost, schedule, and performance impacts:
  - RDT&E costs
  - Procurement costs
  - O&S costs
  - Performance thresholds
  - Schedule thresholds
  - Affordability caps
- Assess the likelihood of the risk being realized
- Conduct analysis periodically to support cost, schedule, and performance risk assessments

Source: Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, Jan 17
How big is the risk and how likely is it to occur?

- Assess likelihood of occurrence
- Identify the possible consequences in terms of technical, schedule, and cost
- Assess consequence
- Identify the risk level in the 5X5 risk reporting matrix

Key Concept: Build the process before applying it!
Risk Analysis (Example)

<table>
<thead>
<tr>
<th>Level</th>
<th>Likelihood</th>
<th>Probability of Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Near Certainty</td>
<td>&gt; 80% to ≤ 99%</td>
</tr>
<tr>
<td>4</td>
<td>Highly Likely</td>
<td>&gt; 60% to ≤ 80%</td>
</tr>
<tr>
<td>3</td>
<td>Likely</td>
<td>&gt; 40% to ≤ 60%</td>
</tr>
<tr>
<td>2</td>
<td>Low Likelihood</td>
<td>&gt; 20% to ≤ 40%</td>
</tr>
<tr>
<td>1</td>
<td>Not Likely</td>
<td>&gt; 1% to ≤ 20%</td>
</tr>
</tbody>
</table>

Note: Underlined values must be tailored for specific programs or risks.

<table>
<thead>
<tr>
<th>Level</th>
<th>Technical Performance</th>
<th>Schedule</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Minimal or no consequence to technical performance</td>
<td>Minimal or no impact</td>
<td>Minimal or no impact</td>
</tr>
<tr>
<td>2</td>
<td>Minor reduction in technical performance or supportability, can be tolerated with little or no impact on program</td>
<td>Able to meet key dates. Slip &lt; 1 month</td>
<td>Budget increase or unit production cost increase (&lt;1% of Budget)</td>
</tr>
<tr>
<td>3</td>
<td>Moderate reduction in technical performance or supportability with limited impact on program objectives</td>
<td>Minor schedule slip. Able to meet key milestones with no schedule float. Slip 1 to 2 months</td>
<td>Budget increase or unit production cost increase (1 to 5% of Budget)</td>
</tr>
<tr>
<td>4</td>
<td>Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success</td>
<td>Program critical path affected. Slip &gt; 2 to 4 months</td>
<td>Budget increase or unit production cost increase (&gt;5 to 10% of Budget)</td>
</tr>
<tr>
<td>5</td>
<td>Severe degradation in technical performance; Cannot meet KPP or key technical/supportability threshold; will jeopardize program success</td>
<td>Cannot meet key program milestones. Slip &gt; 4 months</td>
<td>Exceeds APB threshold (≥10% of Budget)</td>
</tr>
</tbody>
</table>
Lesson Overview

Lesson Plan Status

• Risk Overview
• Risk, Issue, and Opportunity Relationship
• IT Related Risks
• Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
• Lesson Review
When mitigating individual risks:

- Consider the accept, avoid, and transfer options, not just the control option.
- Choose the best mitigation options, then select the best implementation approach for those options.
- Ensure appropriate peers and stakeholders are informed about high-risk items; elevate as needed.
- Include cross-program risks in order to consider the impact of risk mitigation actions on other programs.

Source: Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, Jan 17
Risk Mitigation Options:
Risk Acceptance (and Monitoring)

Conscious decision to accept risk:

- Low likelihood or low consequence risk events where DoD is in best position to manage risk.
- Successful risk assumption depends on identifying specific response actions if risk event occurs and assuring resources are available to implement plan.
- Sometimes risk may be assumed because no feasible mitigation is available.
- Accepting a risk does not mean that it should be ignored.
Risk Mitigation Options: Risk Avoidance

Eliminate source of risk:

- Accomplished by changing concept, specifications, or processes.
- Generally accomplished early in acquisition process but can occur at any time.
- Often involves trade-off decisions during requirements development.
Risk Mitigation Options: Risk Transfer

Transferring aspects of risk to contractor or third party:

- Through contract structures and/or incentives
- Through insurance and bonding requirements
- Transfer of risk must also be economically reasonable
Reduce risk to acceptable level:

- Can be costly and may impact project objectives, such as cost control or schedule performance.

- Examples: Use of modeling & simulation, reviews such as SETRs (System Engineering Technical Reviews), walk-throughs, inspections, and early prototyping.

- Most common handling used in defense programs – reducing risk by trying to manage it with resources.
## Risk Mitigation Plan

1. Identify and lay out the risk handling activities in a sequential manner, using realistic and logical schedule precedence

<table>
<thead>
<tr>
<th>Action</th>
<th>Who</th>
<th>What</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Ensure all risk handling activities:
   a) are clearly defined and jargon free,
   b) are objective and not subjective, and
   c) have specific, measurable outcomes.

3. Assign a planned likelihood and consequence value to each risk handling activity.

4. Estimate the start and finish dates for each risk handling activity.

5. Include the risk handling activities or a subset of these activities in the program IMS.

6. Chart the relationship of risk handling activities, plotting risk level versus time to estimate their relative risk burn-down/reduction contribution.

---

Example: Is the statement “performing a test” an appropriate activity?

---

How about? “brassboard throughput test results met or exceeded all performance thresholds requirements, and the results are approved by the user”
• An instant snapshot of the progress of a risk over time
• Actual progress against the planned reduction of risk levels
• Risk Overview
• Risk, Issue, and Opportunity Relationship
• IT Related Risks
• Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
• Lesson Review
Step 1: Using your risk statement from Exercise 1 and your risk matrix from Exercise 2, identify **detailed steps** (template available at chart 5) that will drive risk to an acceptable level given program constraints and objectives.

Step 2. Using the template on chart 6 develop the “Waterfall Chart” showing how you will burn down the risk.

Step 3: Adjust Risk Matrix Expectation (template at chart 7) consistent with Mitigation Planning.

SEE EXERCISE FOLDER ON STUDENT CD (LSN 07) FOR TEMPLATES
Risk Monitoring - How has the risk changed?

When monitoring risks:

• Track the implementation and progress of the risk mitigation activities, not just the development and planning of the selected strategy.

• Include Technical Performance Measures as an integral activity when monitoring risks after selecting the appropriate risk mitigation strategy.

• Conduct regular status updates to monitor risks for changes to likelihood and/or consequences.

• Document risks that can be retired as well as risks that are still being mitigated to prevent an unnoticed relapse of the retired risk.

• Keep lines of communication open to notify management when ability to mitigate the risk is ineffective.

Source: Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, Jan 17
Example Risk Monitoring and Trend Matrix

Source: Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, Jan 17
• Risk Overview
• Risk, Issue, and Opportunity Relationship
• IT Related Risks
• Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
• Lesson Review
Life-Cycle Risk Management is a structured process
   - Process for risk identification and risk analysis
Risk Management is required and is smart business
   - You have an obligation to tell senior leaders the true program risks
     - Leadership may support risky approach IF high payoff and good risk management strategy
Benefits of Life-Cycle Risk Management:
   - Ensures solid foundation for development of acquisition strategy and program documentation
   - Focuses program resources on critical issues
   - Helps program avoid being in CRISIS-MANAGEMENT mode
Provides a foundation for program risk management execution.
Today we learned to:

Overall: Given a DoD IT/SW acquisition scenario, apply DoD Risk Management (RM) policy in support of the program’s objectives and priorities.

- Define the elements that constitute an effective RM program for an Information Technology (IT) system acquisition.
- Identify the two components of risk.
- Identify how risk, issue, and opportunity management interrelate.
- Identify risks inherent to IT system acquisition.
- Apply the five components of the DOD RM Process Model to a given IT acquisition scenario.