



# ***Risk Management in Systems Engineering***

***DAU Hot Topics Forum  
20 Jun 07***

**Col Rich Hoferkamp**

**Mr. Mike Zsak**

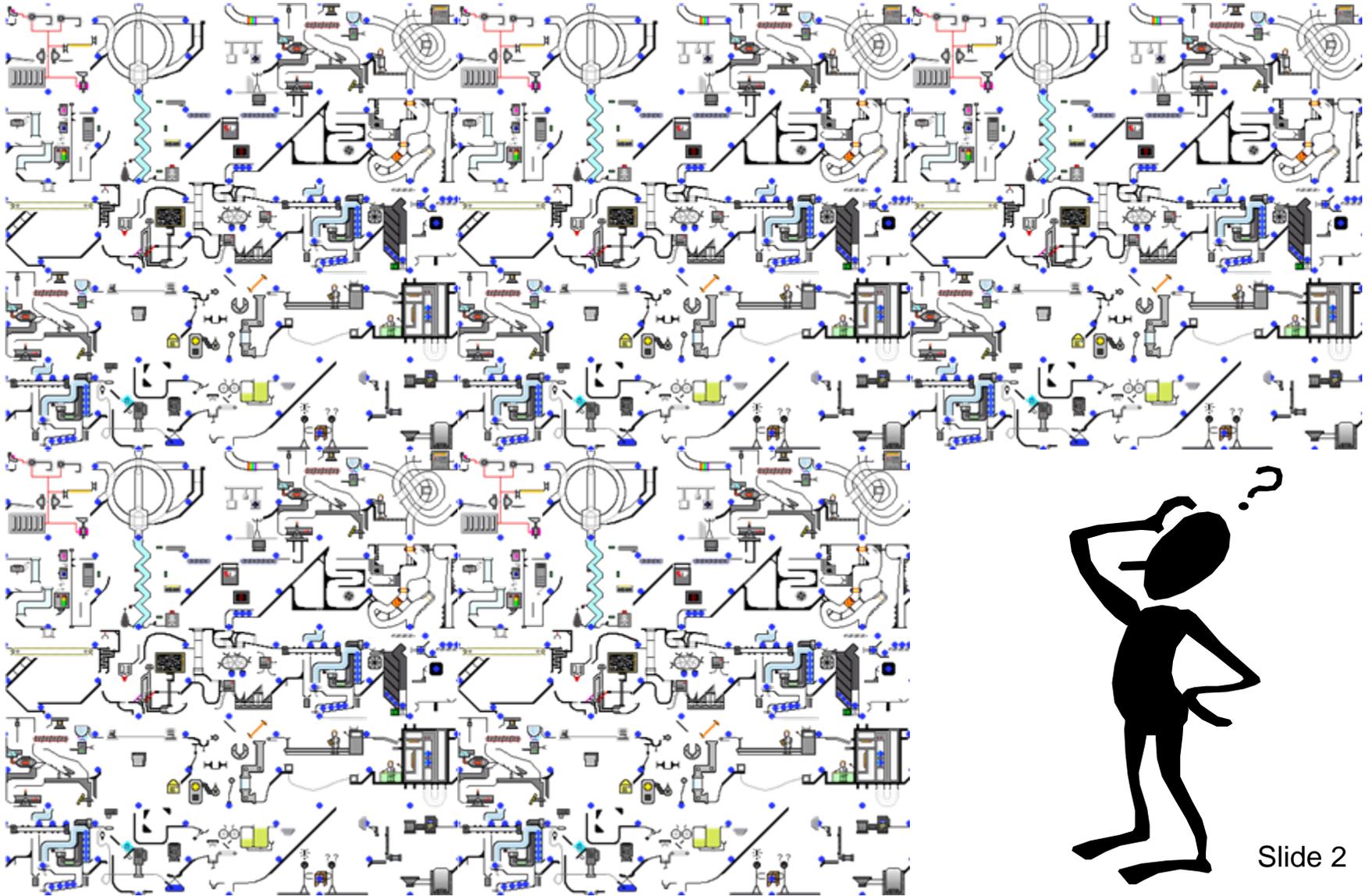
Systems and Software Engineering

(Enterprise Development)

Office of the Under Secretary of Defense (Acquisition & Technology)

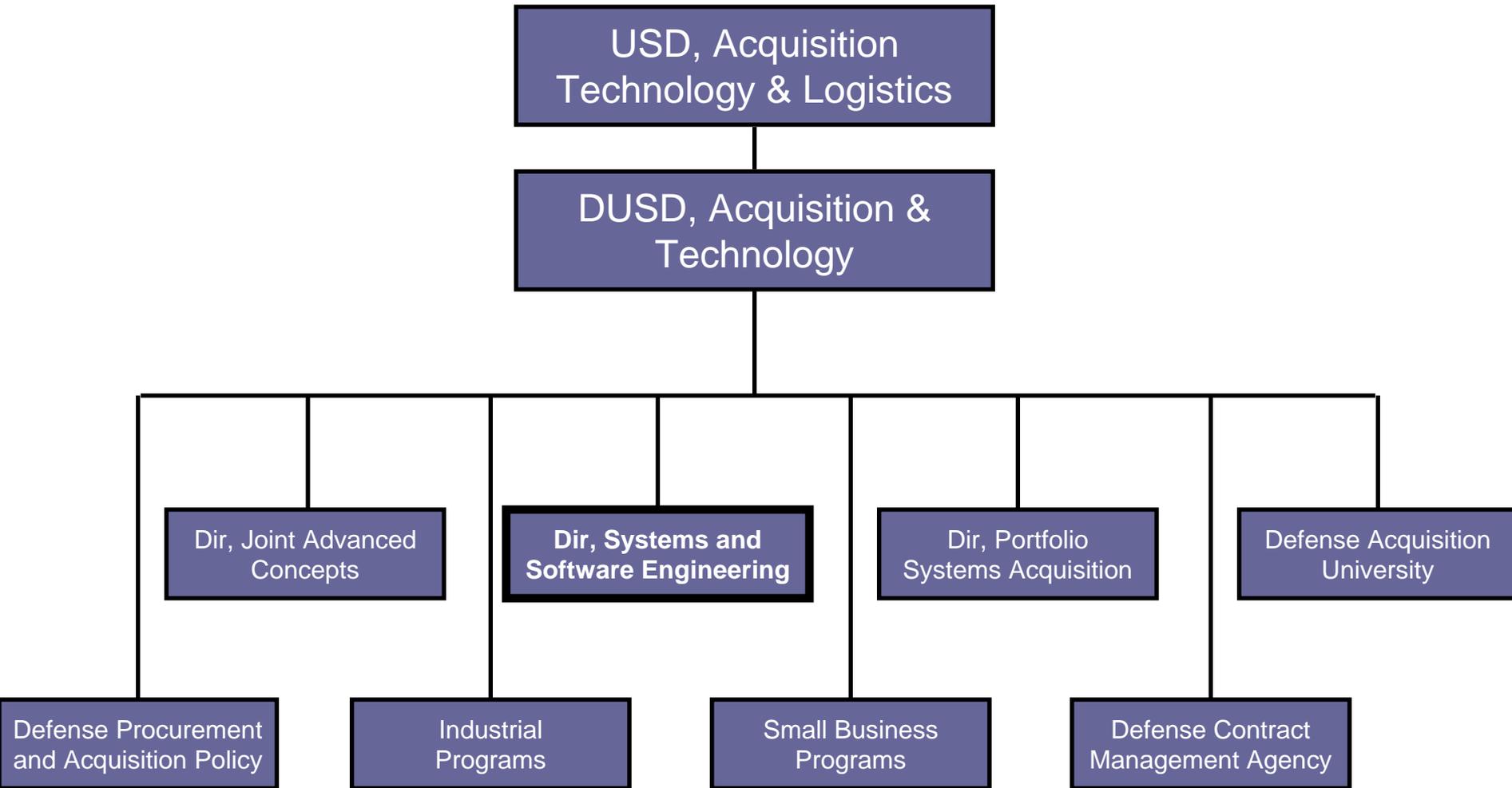


# Risk Management...



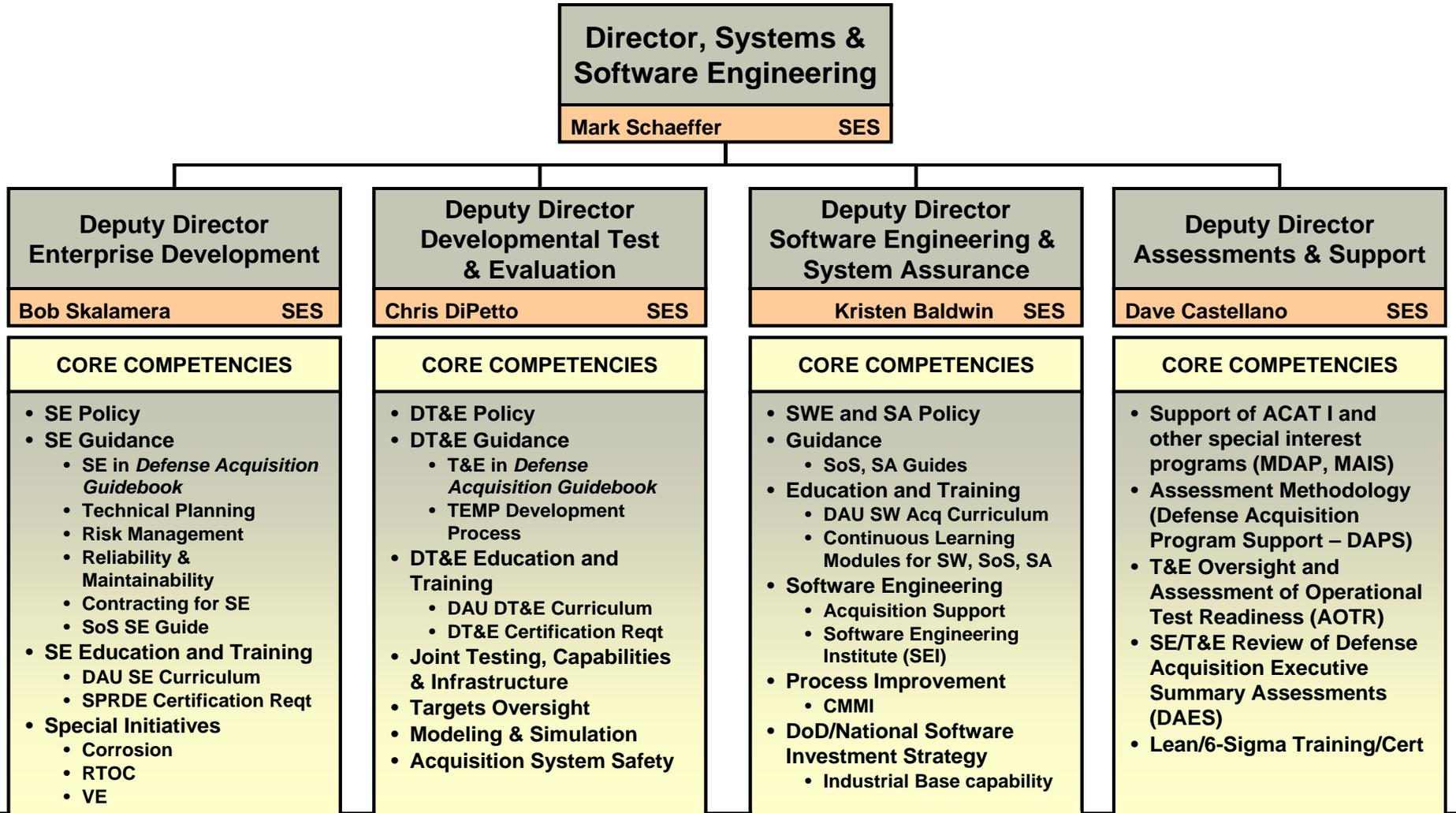


# OUSD (AT&L) Organization





# Systems and Software Engineering Organizational Core Competencies



*Acquisition program excellence through sound systems and software engineering*



# System Engineering Policies

**All programs shall develop a SE Plan (SEP)**

**Each PEO shall have a lead or chief systems engineer who monitors SE implementation within program portfolio**

**Event-driven technical reviews with entry criteria and independent subject matter expert participation**

**OSD shall review program's SEP for major acquisition programs (ACAT ID and IAM)**

**Technical Planning**

**Technical Leadership**

**Technical Execution**

**Technical Excellence**

**Technical planning upfront and early**



# Education & Training

---

## ➤ What's available

- On-line Continuous Learning Modules (CLMs): Reliability and Maintainability; Technical Reviews; Technical Planning
- On-line introductory course SYS 101
- On-line intermediate course SYS 202
- Intermediate classroom course SYS 203
- Advanced classroom course SYS 302
- New "SPRDE/Program Systems Engineer" track

## ➤ What's coming

- Update to Risk Management CLM (and PMT 250 module)
- New CLMs for MOSA (Open Systems), M&S in T&E, and Trade Studies
- "Core-plus" career guidance



# Guidance

---

- What's available:

- *Systems Engineering Plan (SEP) Preparation Guide*
- *Risk Management Guide for DoD Acquisition*
- DoD Guide for Achieving Reliability, Availability, and Maintainability
- Integrated Master Plan/Integrated Master Schedule (IMP/IMS) Guide
- Guide to Integrating SE into DoD Acquisition Contracts
- Understanding and Leveraging a Supplier's CMMI Efforts: A Guidebook for Acquirers
- Systems of Systems SE Guide

- What's coming:

- Update to SEP Preparation Guide
- Update to Defense Acquisition Guidebook
  - Chapter 4 -- Systems Engineering
  - Chapter 9 -- Test and Evaluation



# Systems Engineering Plan

---

- Provides insight into every aspect of a program's technical plan to aid programs in thinking through their SE process and set a firm technical foundation. Five focus areas:
  - Program Requirements
  - Technical Staffing and Organizational Planning
  - Technical Baseline Management
  - Technical Review Planning
  - Integration with Overall Management of the Program
  
- Should be key part of the acquisition strategy/built into RFP
  
- Applicable to all milestones and phases of a program
  - MS A and Technology Development
  - MS B and System Development & Demonstration
  - MS C and Production & Deployment/Operations & Support

**It's about the planning, not the plan**



# Risk Management

---

## ➤ Purpose:

- To help ensure program cost, schedule, and performance objectives are achieved at every stage in the life cycle
  - To communicate to all stakeholders the process for uncovering, determining the scope of, and managing program uncertainties
- Addresses risks associated with all aspects of a program
- Involves all members of IPT, not just the program manager or systems engineer

**Now part of DAES reporting requirements**



# Technical Plan/Risk Management Plan Integration Examples

---

## ➤ Program Requirements

- SEP: describe the critical technologies of the preferred system concept
- Risk: the critical technologies do not mature by MS B
- Mitigation: Adjust driving requirement to accommodate more mature technology

## • Technical Staffing

- SEP: describe your system safety certification requirements
- Risk: the System Safety subject matter expert may retire early
- Mitigation: identify support contractor; initiate cross-training; multiplex across IPTs

## • Technical Baseline Management

- SEP: describe the approach to requirements traceability and verification
- Risk: the Modeling & Simulation software (for verification) underperforms
- Mitigation: plan schedule for regression testing; have provisions to analyze and fix

## • Technology Maturation

- SEP: describe how event-driven Technical Reviews will be conducted
- Risk: political pressure to stay on schedule regardless of technical maturity
- Mitigation: plan for early/continuous tracking of product maturity; build in on/off ramps

## • Integration with Overall Program

- SEP: describe integration of technical planning with test & evaluation plans
- Risk: the window for using the test range is not met
- Mitigation: line up other ranges in advance; explore opportunities for re-sequencing of testing

**Identify risks as part of the technical planning**



# **RISK MANAGEMENT GUIDE FOR DOD ACQUISITION**

**Sixth Edition  
(Version 1.0)**



**August, 2006  
Department of Defense**



# Everyone Wants to Understand Risk





# Risk Management Guide for DoD Acquisition

---

- The new *Guide* places emphasis on:
- The role and management of future root causes
  - Distinguishing between risk management and issue management
  - Tying risk likelihood to the root cause rather than the consequence
  - Tracking the status of risk mitigation implementation vs. risk tracking
  - Event-driven tech reviews to help identify risk areas and assess the effectiveness of mitigation efforts

**Updated Guide reflects lessons learned on the application of risk management on past programs**



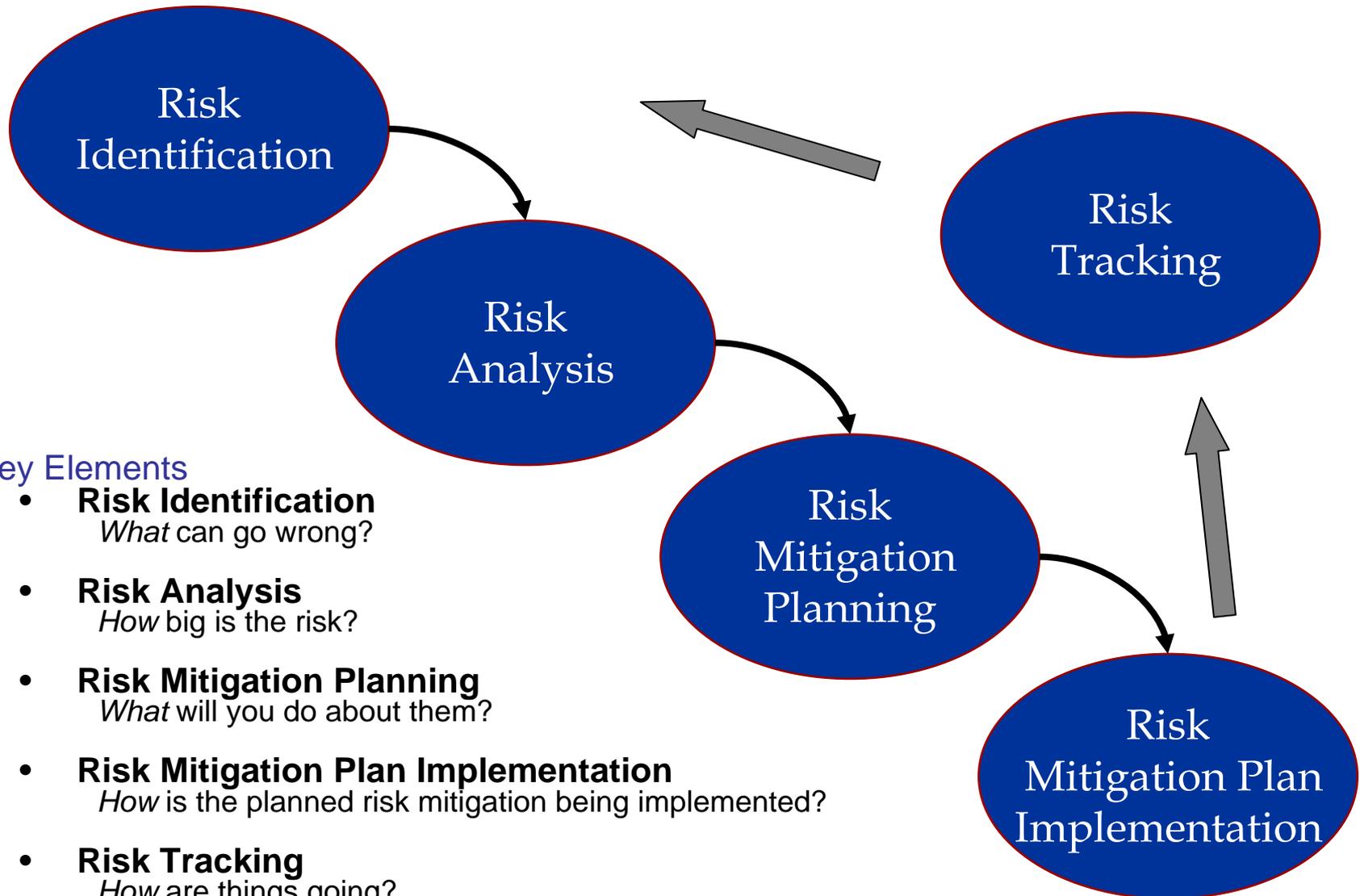
# Risk Management

---

- Risk management is the overarching process that encompasses the risk elements of identification, analysis, mitigation planning, mitigation plan implementation, and tracking



# Risk Management Process Model



## Key Elements

- **Risk Identification**  
*What can go wrong?*
- **Risk Analysis**  
*How big is the risk?*
- **Risk Mitigation Planning**  
*What will you do about them?*
- **Risk Mitigation Plan Implementation**  
*How is the planned risk mitigation being implemented?*
- **Risk Tracking**  
*How are things going?*



# Risk Management: What is Risk?

---

- Risk has three components
  - A future risk root cause
  - A probability (likelihood) of the future risk root cause occurring
  - The consequence (or effect) of the future occurrence



# Risks vs. Issues vs. Opportunities

---

## ➤ Risks: *yet to happen*

- Future consequences
- Can be “closed” only after successful mitigation through avoiding, controlling, transferring, or assuming the risk

## ➤ Issues: *current* problems and/or challenges

- Real-time consequences
- Can be closed within 30-60-90 days windows

## ➤ Opportunities: *yet to happen*

- Future potentially desirable situation or circumstance
- Process for managing similar to risk process

**If it has already occurred, it's an issue, not a risk**



# Why manage RISK?

---

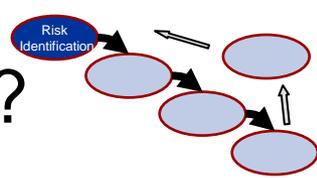
- Ensure program cost, schedule and performance objectives are achieved
- Communicate to all stakeholders the process for uncovering, determine the scope of, and managing program uncertainties

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

**~ Barry Boehm in *Software Risk Management***



# Identifying Risk: What Can Go Wrong?



- An approach for identifying potential risk root causes is to
- List WBS product or process elements
  - Examine each in terms of risk sources or areas
  - Determine what could go wrong
  - Ask “why” multiple times until the root cause(s) is discovered
  - Compile a list of potential risk root causes

**Early and continuously from the time performance requirements are developed**



# Identifying Risk: What Can Go Wrong?



*I cannot imagine any conditions which would cause a ship to founder.*

Captain E.J. Smith, 1906  
(Captain of *Titanic* on the evening on 14 April, 1912)



## Identifying Risk: When Do Risk Root Causes Typically Occur?

---

- From an informal SEI survey
  - During the development process – 33 %
  - When changes are made – 43%
  - When something external to the project changes – 24%

**What is your experience?**



# Identifying Risk: Where to Look for Potential Risks

---

## ➤ Where risks originate

- Technical
- Schedule
- Cost

## ➤ Suggestions

- Examine lessons learned
  - History will repeat itself
- Study the WBS and SOW
  - Be thorough, but not absurd
  - Take care not to focus all your efforts on highly improbable scenarios
  - Use technical reviews to gauge risks to program
- Leverage collaboration, particularly with experts

**What has worked for you?**



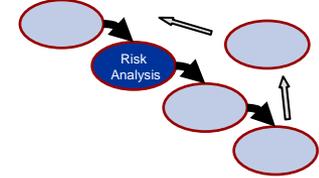
# Identifying Risk: Technical Risk Drivers

---

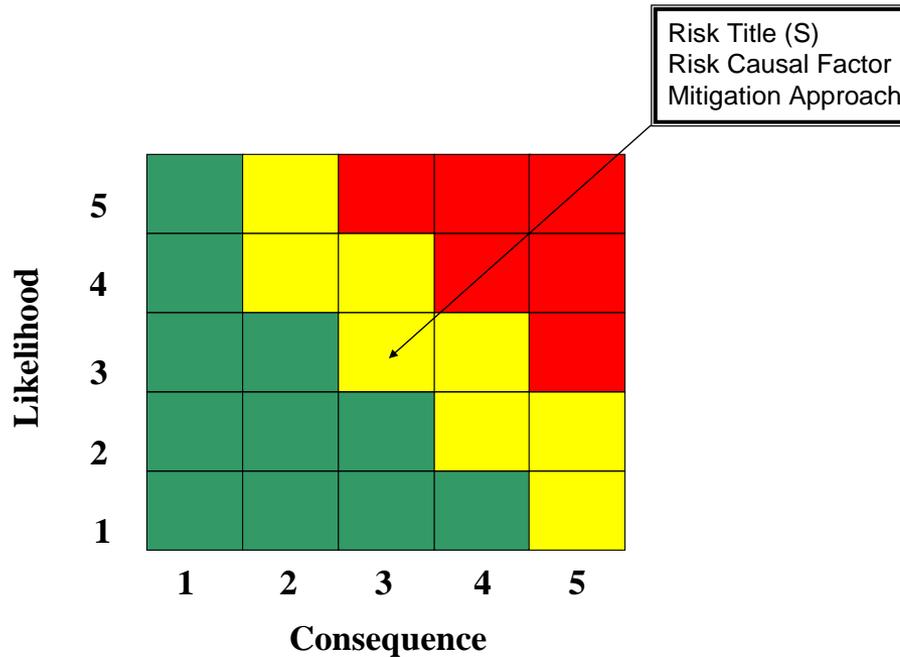
- Requirements
- Complexity
- Size
- Stability
- Support Concepts
- Reliability and Maintenance
- Constraints
- Personnel
- Computer Resources
- Manufacturing Resources
- Standards
- Government Furnished  
Equipment/Personnel
- Environment
- Proprietary Data/Designs
- Technology
- Hardware State-of-the-art
- Software
- Tools
- Data Rights
- Experience
- Developmental Approach
- Process Model
- Process Maturity
- Documentation
- Management Approach
- Integration Approach



# Risk Analysis



- Answer the question, “How big is the risk?”
  - Consider the likelihood of the root cause occurrence
  - Identify the possible consequences in terms of technical, schedule, cost
  - Identify the risk level in the 5X5 risk reporting matrix





# Risk Analysis: Likelihood

	Level	Likelihood	Probability of Occurrence
<b>Likelihood</b>	1	Not Likely	~10%
	2	Low Likelihood	~30%
	3	Likely	~50%
	4	Highly Likely	~70%
	5	Near Certainty	~90%



# Risk Analysis: Consequence

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

\*Tailor for program in month(s)

\*\* Tailor for program in whole dollars



# Biases to Consider When Evaluating Risks (1 of 2)

---

## ➤ Status quo bias

- Strong bias toward alternatives that perpetuate the status quo
  - More choices = increased attraction to status quo

## ➤ Confirming evidence bias

- We seek out information that supports our existing point of view while avoiding information that contradicts it
- Underlying factors
  - Tendency to be engaged more by things we like than dislike
  - Tendency to subconsciously decide what we want to do before we figure out why



## Biases to Consider When Evaluating Risks (2 of 2)

---

### ➤ Anchoring bias

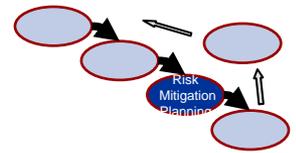
- We tend to give disproportionate weight to the first information we receive
  - Most common anchor: a past event or trend
- Underlying factors
  - Initial impressions, estimates, or data “anchor” subsequent thoughts and judgments

### ➤ Sunk cost bias

- We tend to make choices in a way that justifies past choices
  - Allowing old investments of time/money to influence new decisions
- Underlying factors
  - Failure to admit to past mistakes; failure to recognize previous investments as “unrecoverable”



# Risk Mitigation Planning



- Answering the question: “What is the program approach for addressing this potential unfavorable consequence?”
  - Avoid risk by eliminating the root cause and/or the consequence
  - Control the cause or consequence
  - Transfer the risk, and/or
  - Assume the level of risk and continue on the current program plan

**- What should be done?**

**- When should it be accomplished?**

**- Who is responsible?**

**- How much funding, if any, is required?**





# Risk Mitigation Plans

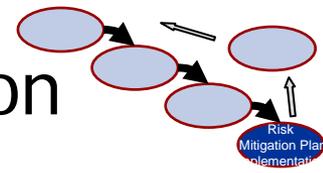
---

- Risk Mitigation plans should contain the following
  - Descriptive title for the risk
  - Date of the plan
  - Risk owner
  - Short description of the risk (including likelihood of occurrence, consequence, etc.)
  - Why the risk exists (root causes)
  - Options for mitigation
  - Status
  - Management recommendation
  - Approvals
  - Resources needed





# Risk Mitigation Plan Implementation



- Answering the question: “How can the planned risk mitigation be implemented?”
  - Determines what planning, budget, and requirements changes are needed
  - Provides a coordination vehicle with management and other stakeholders
  - Documents changes

**IPTs at each WBS level should scrub and endorse the risk mitigations of lower levels**



# Risk Mitigation: Dealing with REALITY

---

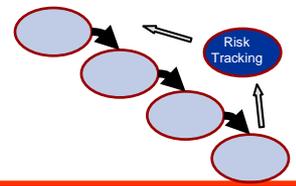
- There's not enough staff time (human hours) or schedule time or funding to address all potential risks
- Which risks are unacceptable?
- Can we avoid or mitigate these?



**Can we live with what we can't fix?  
Will the mitigation strategy work?**



# Risk Tracking



- Answering the question: “How are things going?”
  - Communicate risks to all affected stakeholders
  - Monitor risk plans
  - Review regular status updates
    - Technical reviews 
    - Risk Management Board
    - Displaying risk management dynamics by tracking risk status on risk reporting matrix
    - Generally the likelihood changes, not the consequence

**The key to the tracking process is to establish a management indicator system over the entire program which provides early warning of problems**



# Risk Management Plan (RMP)

---

- Risk planning, and the resultant plan, should answer the questions: “who, what, where, when, and how.”
- Suggested RMP format
  - Introduction
  - Program Summary
  - Risk Management Strategy and Process
  - Responsible/Executing Organization
  - Risk Management Process and Procedures
  - Risk Identification
  - Risk Analysis
  - Risk Mitigation Planning
  - Risk Mitigation Implementation
  - Risk Tracking

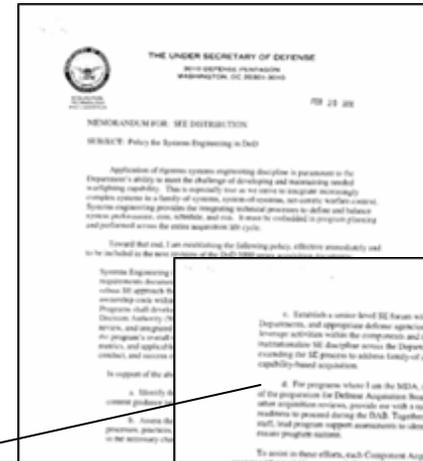




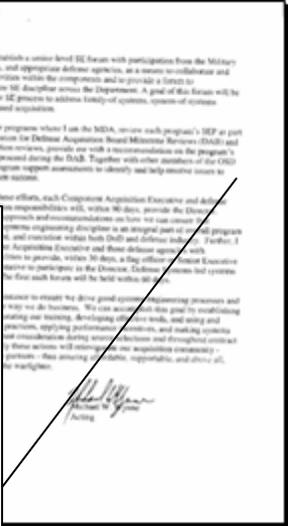


# Program Support Reviews

## USD(AT&L) Imperatives



d. For programs where I am the MDA, review each program’s SEP as part of the preparation for Defense Acquisition Board Milestone Reviews (DAB) and other acquisition reviews, provide me with a recommendation on the program’s readiness to proceed during the DAB. Together with other members of the OSD staff, lead program support assessments to identify and help resolve issues to ensure program success.



➤ § 3.10.5. Program Support Reviews. PSRs mandated for all MDAPs and “. . . shall be conducted prior to each milestone event, before approval of the SDD acquisition strategy, and at other times as directed by the USD(AT&L).”

Source: Draft DoDI 5000.2

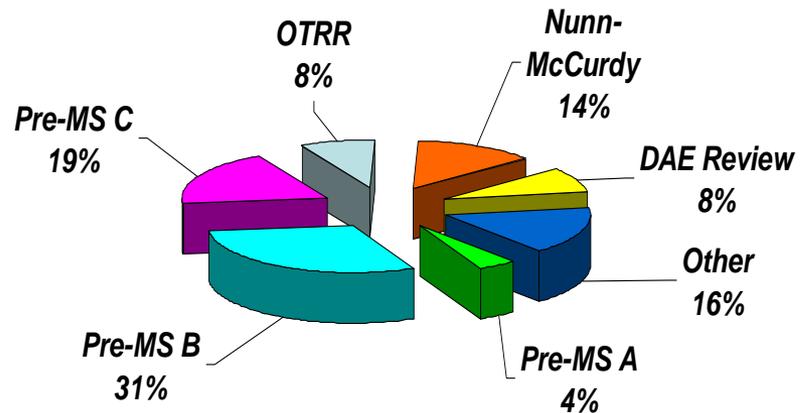


# Program Support Review Activity

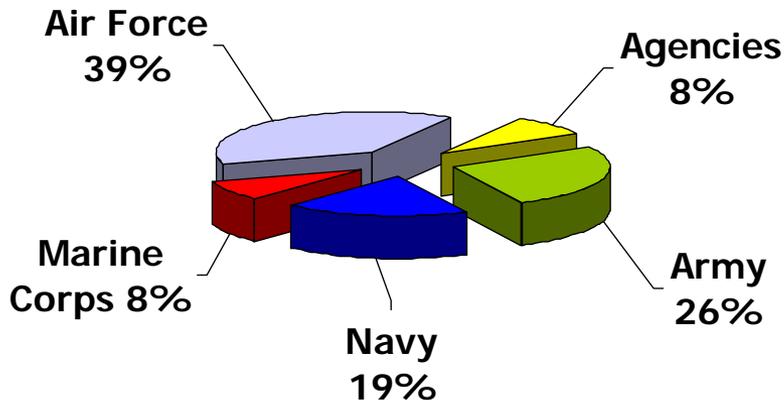
(since March 2004)

- PSRs/NARs completed: 42
- AOTRs completed: 10
- Nunn-McCurdy Certification: 10
- Participation on Service-led IRTs: 2
- Technical Reviews: 9
- Reviews planned for FY07:
  - PSRs/NARs: 10
  - AOTRs: 1
  - Nunn-McCurdy: 6

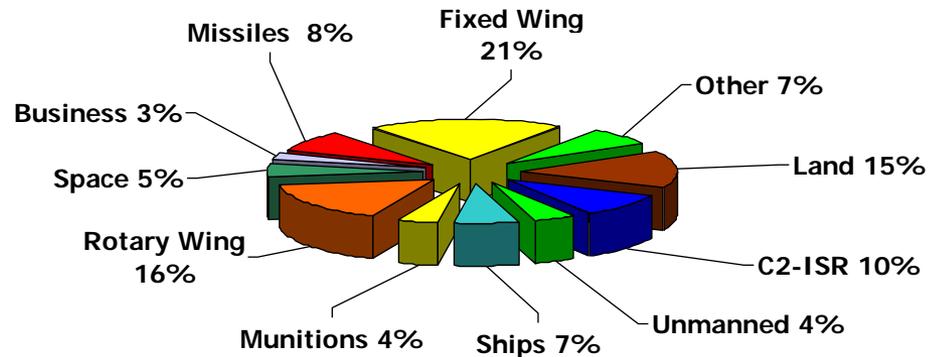
## Decision Support Reviews



## Service-Managed Acquisitions



## Programs by Domain Area





# Common Risk Pitfalls

---

- Programs lack properly documented risk management activities
  - No Risk Management Plan that documents an organized, comprehensive and interactive strategy for managing risk
  - Lack of formal documented risk mitigation plans
    - No mitigation plans for all medium / high risks
  - Lack of off-ramps for major program risks
  - Mitigation tasks do not have resources assigned nor due dates nor the status of the task
  
- Programs lack a mature risk management program 
  - Risk avoidance lessons learned are not addressed within risk management approach
  - Risk management by PMO lacks discipline, effectiveness
  - Mixing of issues and risks



# Common Risk Pitfalls

---

- Tools and methodology supporting risk management are not sufficient
  - Lack of evidence of linkage between TPMs/EVM/Risk Management/WBS/IMS to effectively employ them as management tools that enable risk reduction
  - Risk tool does not map risks to applicable WBS element
  - Government and contractor risk tools are not compatible
  
- Program management does not have a portfolio view of risk management
  - Enterprises do not have a portfolio view of risk management to prevent one program from being adversely impacted by other acquisition programs or enterprise-wide challenges

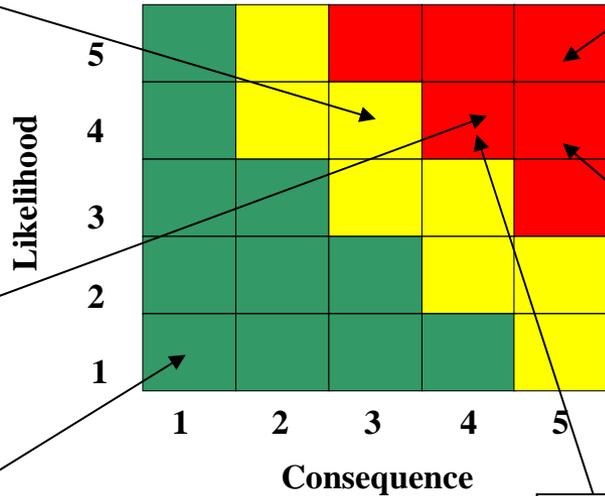


# Risk Reporting 5 X 5 Matrix

**Program Affordability**  
 Additional scope and EAC growth may grow  
 Costs beyond the program budget  
**Mitigation Plan**  
 1. Identify cost reduction baseline  
 2. Identify CAIV trade options

**Range Performance**  
 System weight targets may not be achieved,  
 Causing impacts to system performance  
 and non-compliance requirements  
**Mitigation Plan**  
 1. Establish weight management program  
 2. Substantiate weight estimates  
 3. Identify alternative design solutions or trades

**Engine Exhaust**  
 Current aircraft experiences fuselage heating  
 due to exhaust impingement  
**Mitigation Plan**  
 1. Local thermal blanketing  
 2. Trade study for redirection of exhaust



**Inspection**  
 Short Interval (100 hour) inspections for bushing wear and hub cracking will increase overall system down-time and increase spares requirement  
**Mitigation Plan**  
 1. Additional spares  
 2. Accelerate new development  
 3. Establish retrofit plan option

**Increment 1 Impact on IOC**  
 IOC may be delayed beyond Threshold dates  
**Mitigation Plan**  
 1. Mitigate SETR delays through out of station mods  
 2. Optimize production, missionization and T&E

**Inc 1 & 2 Configuration Differences**  
 Inc 2 requirements may drive unique differences resulting in Inc 1 structures not being unusable for Inc 2  
**Mitigation Plan**  
 1. Identify structural retrofit requirements  
 2. Identify potential requirement trades  
 3. Determine technical, schedule and cost viability of retrofit



# Challenges\*

---

- **Instituting risk management as a normal PM activity in DoD**
- **Demonstrating that risk management improves changes for program success**
- **Showing that risk management gives significant benefits at small cost**
- **Providing meaningful help to all levels of programs**
- **Communicating realistic risk levels throughout entire program community**

**How are we doing?**

\* Source: DSMC Risk Management Workshop, June 1998



# Risk Management Everybody's Business

---



## **BUT, BE AWARE:**

Risks Happen!

Identifying and dealing with them will make life easier in the long run  
It's a team effort, no matter what your role, you need to be part of the team  
All stakeholders **MUST** be involved!



# Risk Realization – Bad News

---

**“Bad news isn’t wine. It doesn’t improve with age.”**

**Colen Powell**



# SE Links

---

## Guides

<http://www.acq.osd.mil/se/publications.htm>

## Education & Training

<http://www.dau.mil/basedocs/trainingcourses.asp>

## Risk Management

<https://acc.dau.mil/rm>



---

# Back-up

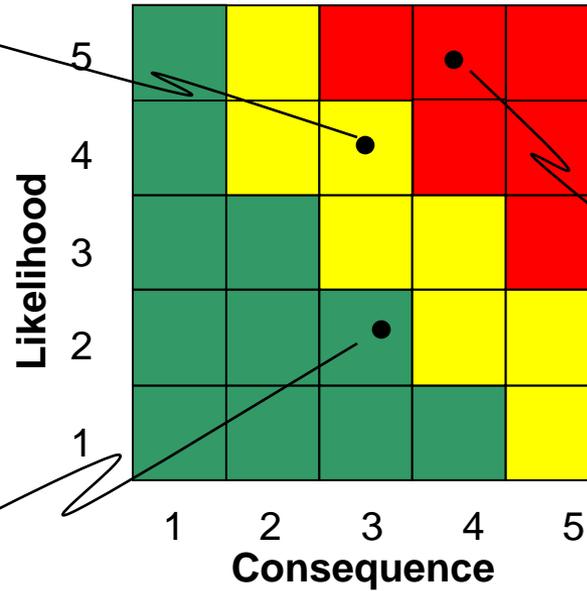


# Risk Summary (Chart 3)

Program Name: \_\_\_\_\_

Date: \_\_\_\_\_

- Risk:
- Driver:
- Mitigation:
- Date:



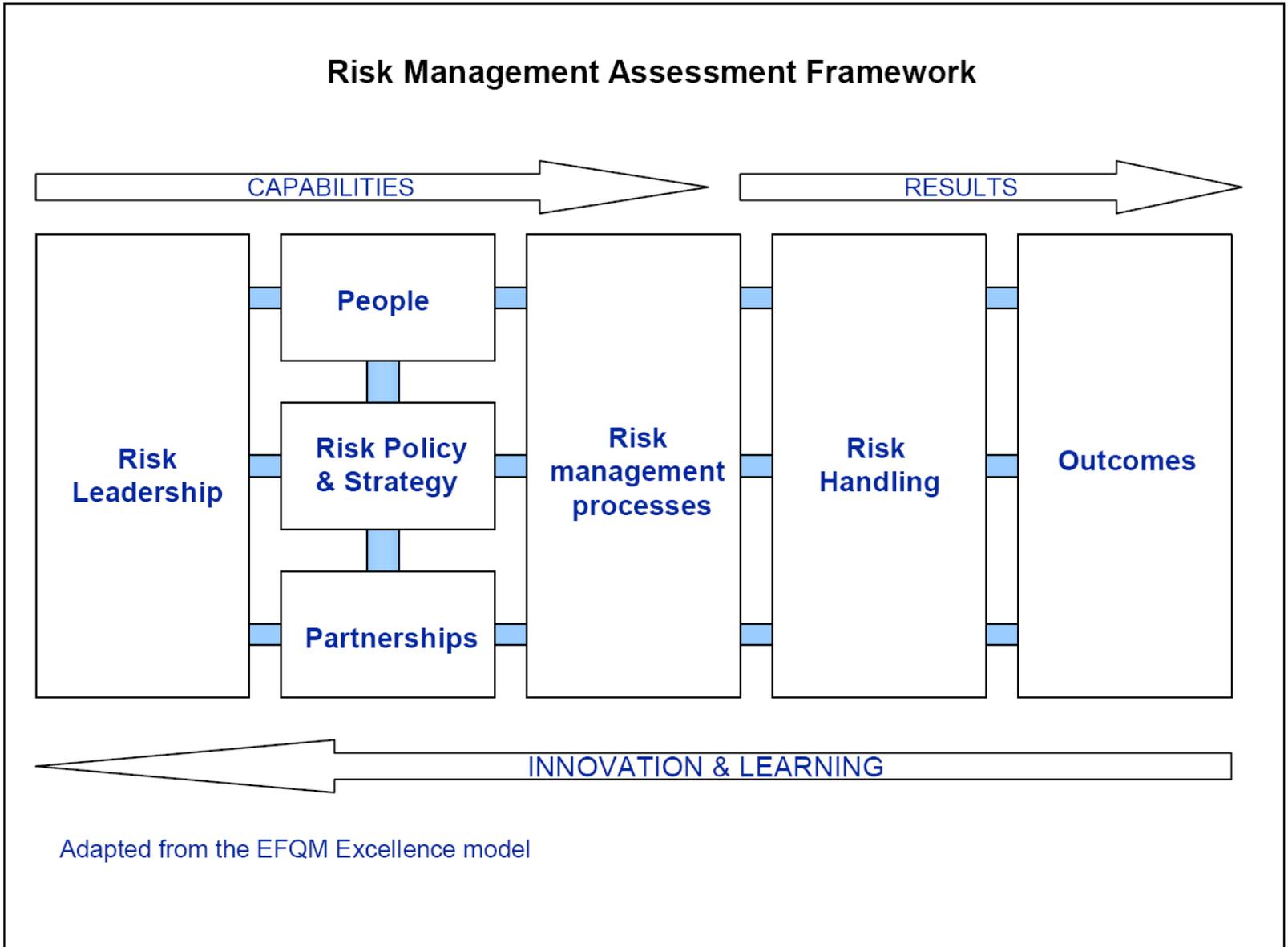
- Risk:
- Driver:
- Mitigation:
- Date:

- Risk:
- Driver:
- Mitigation:
- Date:

Pre-Decisional



# UK Risk Management Assessment Tool





# UK Risk Management Assessment Tool

## Leadership

Level 1: <input type="checkbox"/> Awareness & understanding	Level 2: <input type="checkbox"/> Implementation planned & in progress	Level 3: <input type="checkbox"/> Implemented in all key areas	Level 4: <input type="checkbox"/> Embedded and improving	Level 5: <input type="checkbox"/> Excellent capability established
Top management are aware of need to manage uncertainty & risk and have made resources available to improve	Senior Managers & Ministers take the lead to ensure that approaches for addressing risk are being developed and implemented	Senior Managers act as role models to apply risk management consistently and thoroughly across the organisation	Top down commitment with embedding and integrating risk management as routine business practice	Senior Managers re-enforce and sustain risk capability, organisational & business resilience and commitment to excellence. Leaders invited to speak at conferences about their success

## Risk strategy and policies

Level 1: <input type="checkbox"/> Awareness & understanding	Level 2: <input type="checkbox"/> Implementation planned & in progress	Level 3: <input type="checkbox"/> Implemented in all key areas	Level 4: <input type="checkbox"/> Embedded and improving	Level 5: <input type="checkbox"/> Excellent capability established
The need for a risk strategy and related policies has been identified and accepted	A risk management strategy & policies have been drawn up and communicated and are being acted upon	Risk strategies & policies are communicated effectively and made to work through a framework of processes	A separate risk strategy and policies not necessary; Risk handling is an inherent feature of all policies and strategy making processes	Risk management capability in strategy and policymaking helps to drive the risk agenda and is reviewed and improved. Role model status

## People

Level 1: <input type="checkbox"/> Awareness & understanding	Level 2: <input type="checkbox"/> Implementation planned & in progress	Level 3: <input type="checkbox"/> Implemented in all key areas	Level 4: <input type="checkbox"/> Embedded and improving	Level 5: <input type="checkbox"/> Excellent capability established
Key people are aware of the need to assess and manage risks and they understand risk concepts and principles	Suitable guidance is available and a training programme has been implemented to develop risk capability	A core group of people have the skills & knowledge to manage risk effectively	People are encouraged and supported to be more innovative. Regular training is available for people to enhance their risk skills	All staff are empowered to be responsible for risk management and see it as an integrated part of the Departments business. They have a good record of innovation and well managed risk taking



# UK Risk Management Assessment Tool

## Partnerships

Level 1: <input type="checkbox"/> Awareness & understanding	Level 2: <input type="checkbox"/> Implementation planned & in progress	Level 3: <input type="checkbox"/> Implemented in all key areas	Level 4: <input type="checkbox"/> Embedded and improving	Level 5: <input type="checkbox"/> Excellent capability established
Key people are aware of areas of potential risk with partnerships and understand the need to agree approaches to manage these risks	Approaches for addressing risk with partners are being developed and implemented	Risk with partners is managed consistently for all key areas and across organisational boundaries	Sound governance arrangements established, partners & suppliers selected on basis of risk capability & compatibility	Excellent arrangements in place to identify and manage risks with all partners and to monitor and improve performance. Organisation regarded as a role model

## Processes

Level 1 <input type="checkbox"/> Awareness & understanding	Level 2: <input type="checkbox"/> Implementation planned & in progress	Level 3: <input type="checkbox"/> Implemented in key areas	Level 4: <input type="checkbox"/> Embedded and improving	Level 5: <input type="checkbox"/> Excellent capability established
Some stand-alone risk management processes have been identified	Recommended risk management processes are being developed	Risk management processes implemented in key areas. Risk capability self assessment tools used in some areas	Risk metrics are collected. Risk management standards applied in some areas	Management of risk & uncertainty is well integrated with all business processes. Best practice approaches are used and developed. Selected as a benchmark site by other organisations





# SEP Prep Guide

---

- Update to be completed by 30 June 07
- New guide includes sections by program phase:
  - Technology Development
  - System Development & Demonstration
  - Production & Deployment and Operations & Support
- Each section is based on technical planning focus areas for that phase
  - Program Requirements
  - Technical Staffing
  - Technical Baseline Management
  - Technical Review Planning
  - Integration with Overall Management of the Program



# Technical Review Risk Assessment Checklists

---

- Acquisition program risk assessments are conducted via event-driven technical reviews to ensure critical performance, schedule, and life-cycle cost risks are addressed, with mitigation actions and budget projections incorporated into program planning
  - These event-driven technical reviews are not the place for problem solving, but to verify that problem solving has been accomplished
- A separate checklist is available for each of 18 technical reviews [including technology readiness assessments and technology dependent (IBR and OTRR) program reviews]
- The checklists assist in the preparation for, and conduct of event-driven technical reviews, and are used as the primary guide for the risk assessment during each review
  - Each checklist contains a bank of questions designed to address all relevant subjects/disciplines
  - Responses on the digital checklist are automatically tallied and summarized
- Checklists are available on SE COP at <https://acc.dau.mil/SE> and in the DAU *Technical Reviews* Continuous Learning Module, CLE-003, available at <http://clc.dau.mil>.



# Technical Review Risk Assessment Checklists

---

## ➤ Recommended practices

- Immediately following completion of the prior review, each technical IPT lead should review the checklist for the next sequential review
- In conjunction with pre-defined (SEP, ADM, etc.) technical review entry criteria, successful completion of each checklist will ensure a successful, non-controversial technical review, thus authorizing the program to move forward
- Generally, the results of the risk assessment checklists (completed before the actual conduct of the review) are utilized during the technical review
  - Typically only high and moderate risks are reviewed in detail
- Some technical review board chairpersons prefer to complete the risk assessment checklist during conduct of the review
  - May be advantageous if the checklist was not completed during preparation for the review, but generally takes more time, and frequently reveals shortcomings in preparation for the review



# TRR Checklist

**“Systems Engineering for Mission Success”**

**Test Readiness Review  
Program Risk Assessment Checklist** (17 May 2007 version)

**OVERVIEW:** Although the checklist can be printed and completed as a “hard copy”, it is designed to be completed electronically as an Excel spreadsheet. When viewed electronically, the small number buttons in the upper left corner of the screen are used to select the level of indenture for the questions in the checklist. A left mouse click on a number button will expand or collapse the entire checklist to the desired level. A left click on the “+” symbol in the left margin of the spreadsheet will expand the level of indenture for that section. A left click on the “-” symbol in the left margin of the spreadsheet will collapse the level of indenture for that section. The buttons in Row 11 run specific macros. The buttons in Column A allow a user to designate and sort specific questions as “Special Interest” (i.e., High Priority, Flagged, Question). The colored buttons in Row 11, Column C allow the user to sort questions by Technical Discipline, to provide a Level 1 roll-up of the risk characters assigned, or to hide specific information. For example selecting the “Logistics” button results in the display of all Level 1 Logistics-related questions and assigned information. All other questions will be hidden.

**COMPLETING THE CHECKLIST:**

- In the upper right corner of the checklist, enter the name of the program being reviewed, the date(s) of the review, along with the name, technical specialty of the person(s) completing the checklist.
- A “Risk Character” (i.e., R/Y/G/U/NA) should be assigned for each question by direct entry or left clicking in each box to activate the “down” menu. The assigned Risk Characters will automatically total and display in the Level 1 (and Level 2, as applicable) row(s). Select a summary tab (Excel “Sheet”) at the bottom of the checklist will provide a summary of all questions assigned a particular risk character (e.g. the RED tab will display all questions assigned a RED risk character). To delete a “Risk Character” from a box, in the box and press the “f” button on the keyboard.
- Any question requiring further attention (Special Interest) should be similarly marked in Column A as “High Priority”, “Flagged”, or “Question” to facilitate follow-up.

**CAUTION:** Entries, changes, deletions or comments should only be made on the checklist. Any entries entered directly on the summary pages will not be recorded within the checklist and will disable linkage between the checklist.

**SAVING THE CHECKLIST:** Save the completed checklist in a new file with a unique name such as “UAV TRR 8Feb07ajo”.

High Priority

Flagged

Question

Show All

Level 1

Programmatic

Production

Interoperability

Technology

Software

Risk

Logistics

Training

EVM

T&E

HSI

Hide TD

Unhide TD

Hide NA

Unhide NA

**Risk Character**  
R = Red, Y = Yellow, G = Green, U = Unknown / Unavailable, NA = Not Applicable

Special Interest	Technical Discipline	Item	R	Y	G	U	NA	Comments / Mitigation
	Level 1, software, programmatic, T&E, logistics, ...	6. Management Metrics Relevant to Planned Test	0	0	0	0	0	

TRR
Red
Yellow
Unknown
NA
Level 1

Filter Mode NUM







# Reality Example

OBJECTIVE – To travel from A to B in time for an important meeting								
RISK	Inherent assessment		CONTROLS IN PLACE	Residual assessment		ACTION PLANNED	TARGET DATE	OWNER
	Impact	Likelihood		Impact	Likelihood			
Missing a train makes me late for the important meeting	High	High	Catch train one earlier than I actually need	High	Low	No further action planned		M.Y. Self
Severe weather prevents the train from running	High	Low	Cannot control	High	Low	Telephone conferencing facility to be installed as a contingency	August	A.N. Other
Engineering works make the train late	High	Medium	Check for engineering works and arrange flexibility with people I am meeting	Medium	Low	No further action planned		M.Y. Self

Source: Management of Risk – Principles and Concepts, Published by the UK HN Treasury, Oct 04