

RISK MANAGEMENT OVERVIEW



Professor Seth Shepherd
Systems Engineering/Test Department
Defense Acquisition University (DAU) – South Region
seth.shepherd@dau.mil
256-922-8751



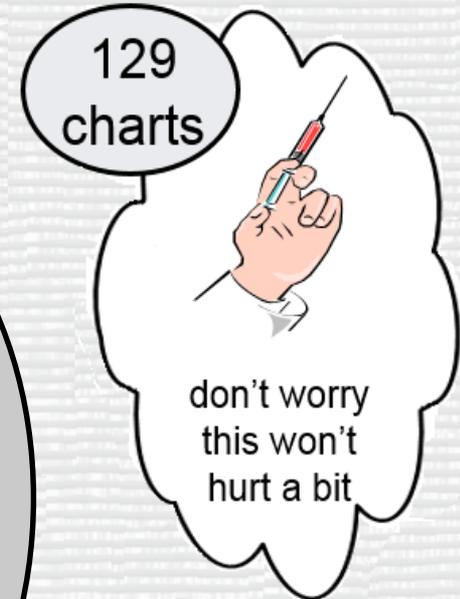
November 4, 2015

www.DAU.mil

LUNCH AND LEARN EXPECTATIONS

- DoD Risk Management Guidance
- Risk Management
 - Risk Planning
 - Risk Identification
 - Risk Analysis
 - Risk Handling
 - Risk Monitoring
- Issue Management
- Opportunity Management
- DAU Risk Management Workshop

Charts contain a lot of detail which is NOT intended to be digested, rather available for deeper discussion or reference.



QUOTES FROM AT&L

- Our task as managers involves optimization—what are the highest-payoff **risk-mitigation investments** we can make with the resources available?
- I expect our managers to demonstrate that they have **analyzed** this problem and made good judgments about how best to use the resources they have to **mitigate** the program's **risk**.

From the Under Secretary of Defense for Acquisition, Technology, and Logistics



Risk and Risk Mitigation—
Don't Be a Spectator

Frank Kendall

Chap 6. PROGRAM MANAGEMENT RESPONSIBILITIES.

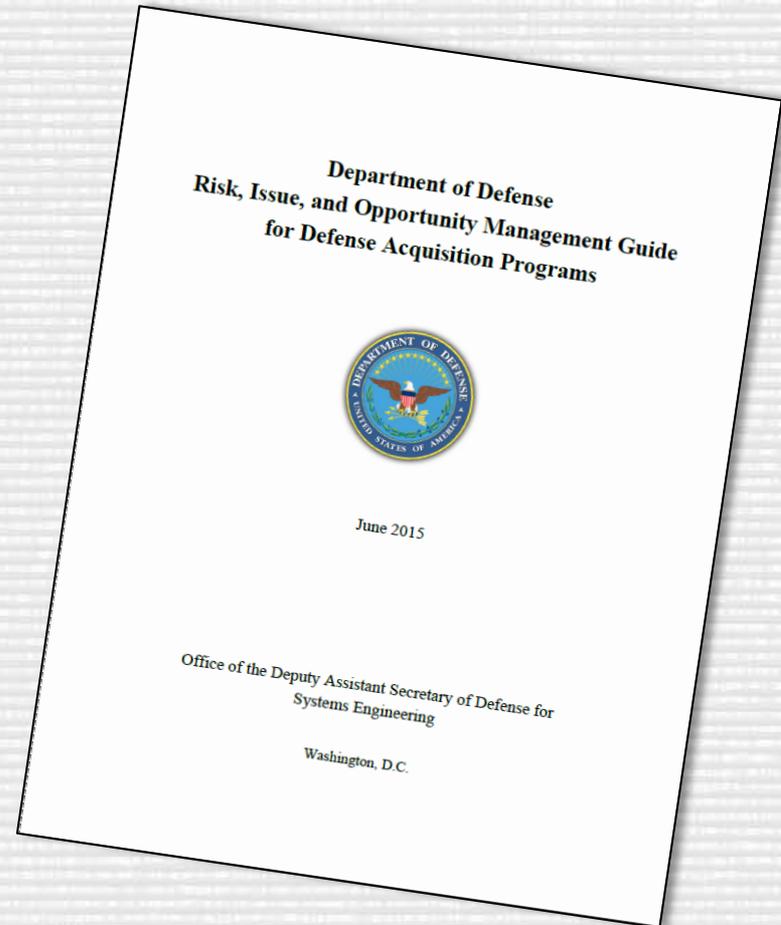
d. Risk Management

(1) The Program Manager is responsible for implementing effective risk management and tracking to include the identification of all known risks, **key assumptions**, probability of occurrence, consequences of occurrence (in terms of cost, schedule, and performance) if not mitigated, **analysis of mitigation options, decisions about actions to mitigate risk, and execution of those actions.**

Risk management is proactive and should be focused on the actions that will be taken and resources that will be allocated to reduce both the likelihood and consequences of risks being realized. Effective risk management is not just risk identification and tracking.

DOD RISK MANAGEMENT GUIDE

- Significantly different from DoD Risk Management Guide, Version 6.0, 2005
- Version 7.0 Published INTERIM in December 2014
- Significantly revised and extended to incorporate comments from the Services, Agencies and DAU
- DRAFT (not for distribution) released for further edit May 2015
- Final Publication of Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs: June 2015



Risk Management Overview



RISK MANAGEMENT

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

Colin Powell



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

Principles of Software Engineering Management Tom Gilb



RISK MANAGEMENT – EVERYONE’S JOB!

Scope

The practice of risk management draws from many management disciplines, including (but not limited to) program management, systems engineering, requirements definition, earned value management, production planning, quality assurance, logistics.

... risk, issue, and opportunity management should be forward-looking, structured, continuous, and informative... must be tailored to the scope and complexity of each program’s needs.

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



RISK MANAGEMENT OBSTACLES

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?



RISK DEFINITION

Risk is the combination of

- (1) the probability of an undesired event or condition and
- (2) the consequences, impact, or severity of the undesired event, were it to occur.*



The undesired event may be programmatic or technical, and either internal or external to the program.

* DoD Risk, Issue, and Opportunity Management Guide June 2015



SOUND RISK MANAGEMENT

- 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



MORE AT&L QUOTES ON RISK

Risk management is not a passive activity, and proactive risk-management investments are not free.

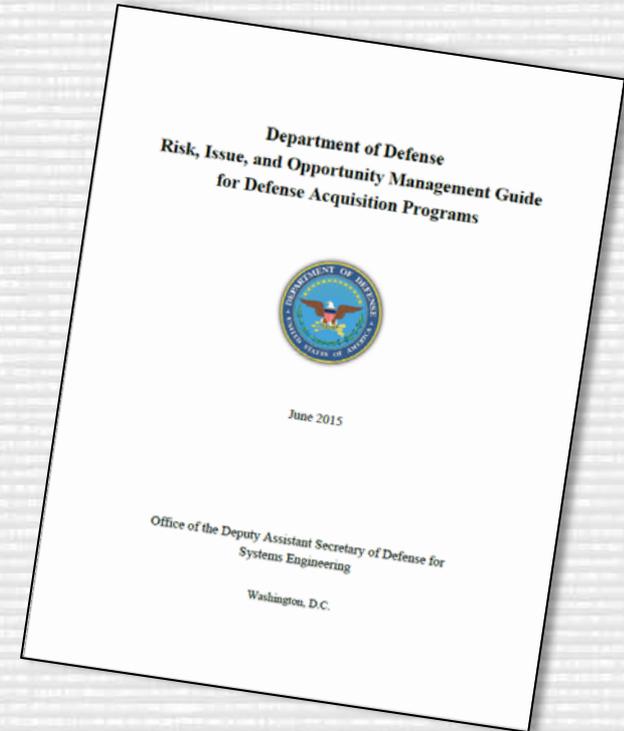
- Those investments, however, can be the most important resource allocations we make in our programs.
- As managers, we need to attack risk the way we've been attacking cost. Understand risk thoroughly, and then go after the risk items with the highest combined likelihoods and consequences and bring them under control.
- Allocate your scarce resources so you achieve the highest possible return for your investments in risk reduction.
- Do this most of all at the very start of program planning.

The course set then will determine the direction of the balance of the program and whether it succeeds or fails.



DOD RIOM CONTENT

- Section 1: Introduces the scope and changes
- Section 2: Describes planning & documentation of program's risk management process.
- Section 3: 5-step risk management process: planning, identification, analysis, handling, and monitoring
- Section 4: Integrating risk management with other program management tools e.g. WBS, IMP, IMS. Metrics e.g. SRA, CRA, PRA, and TPMs.
- Section 5: Issue Management - differentiates between Risk and Issue Management
- Section 6: Opportunity Management
- Section 7: Internal and external interfaces with interdependent programs and cross-program risks.
- Appendixes: Life Cycle Considerations, Activities, Templates, Roles, Responsibilities & Relationships; Risk Management Vignette



RISKS AND ISSUES

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

- Can be “closed” only after successful handling through avoiding, mitigating, transferring, or accepting (assuming) the risk
- Examples:
 - IF the sole source provider of a critical component goes out of business, THEN the program will be delayed by 6 months
 - IF proprietary interfaces are used, THEN maintenance and support costs will likely increase as the program matures

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

- If the probability of occurrence is “near certainty” or if it has already occurred, it’s an issue
- Examples:
 - Release of engineering drawings is behind schedule
 - Test failure of components reveals a design shortfall

If it has already occurred, it’s an **ISSUE**, not a **RISK**



SUCCESSFUL RISK MANAGEMENT

Successful risk management requires thoughtful planning and resourcing, and should be implemented as early as possible in the life cycle. The goal is to identify risks to inform decisions and handling strategies before they become issues.

**RISK or
ISSUE ?**



**RISK
or
ISSUE ?**



RISK MANAGEMENT APPROACH

It is essential that programs define, implement, and document an appropriate risk management approach that is organized, comprehensive, and iterative by addressing the following questions:

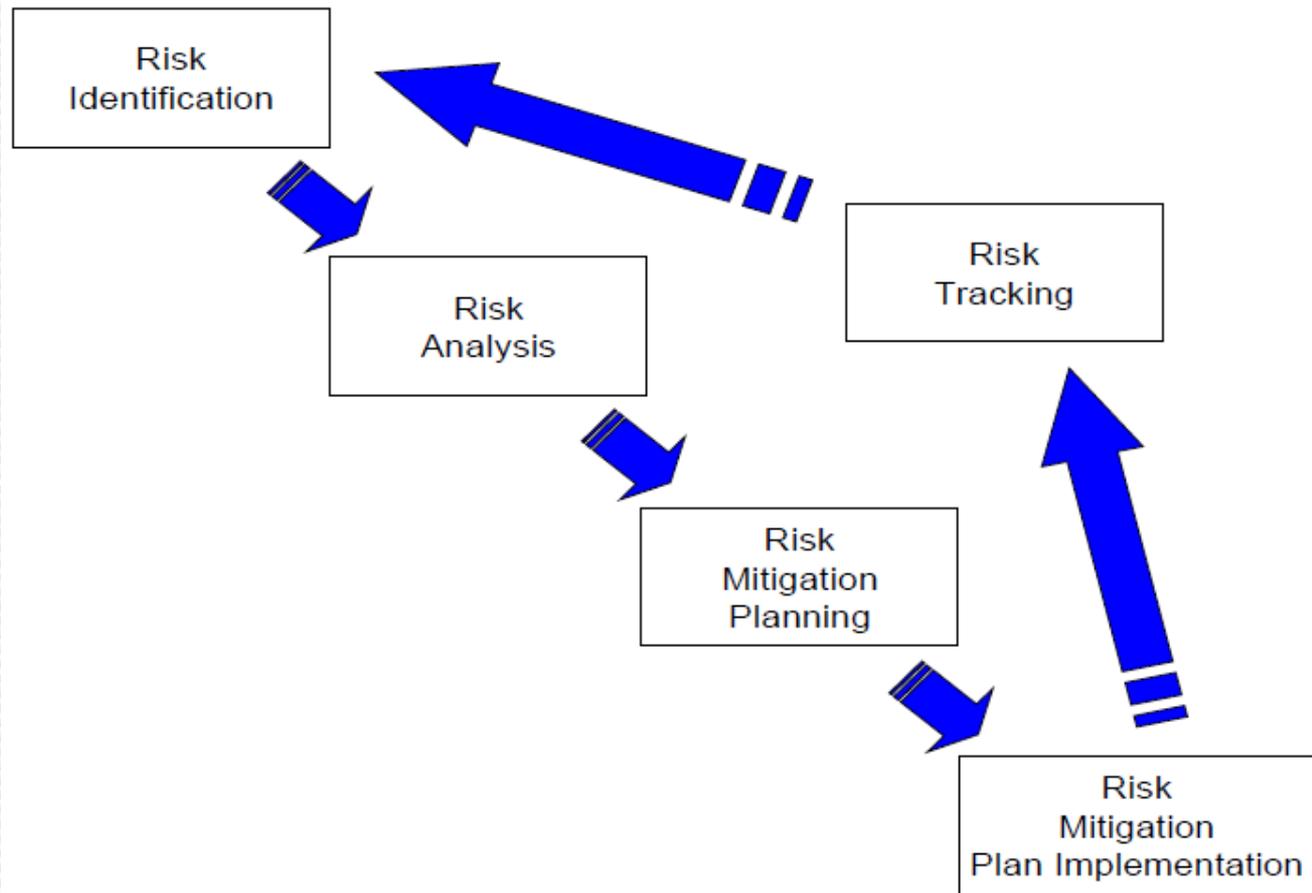
- Risk Planning: What is the program's risk management process?
- Risk Identification: What can go wrong?
- Risk Analysis: What is the likelihood and consequence of the risk?
- Risk Handling (**Mitigation**): Should the risk be accepted, avoided, transferred, or mitigated?
- Risk Monitoring (**Tracking**): How has the risk changed?



Changes
from
previous
language



2005 RISK MANAGEMENT APPROACH



DOD Risk Management Guide 6th Edition, Aug 2005



2015 RISK MANAGEMENT APPROACH



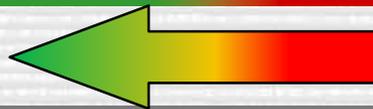
DoD Risk, Issue, and Opportunity Management Guide June 2015



ALTERNATIVE TO RISK MANAGEMENT

Risk Management vs. Crisis Management

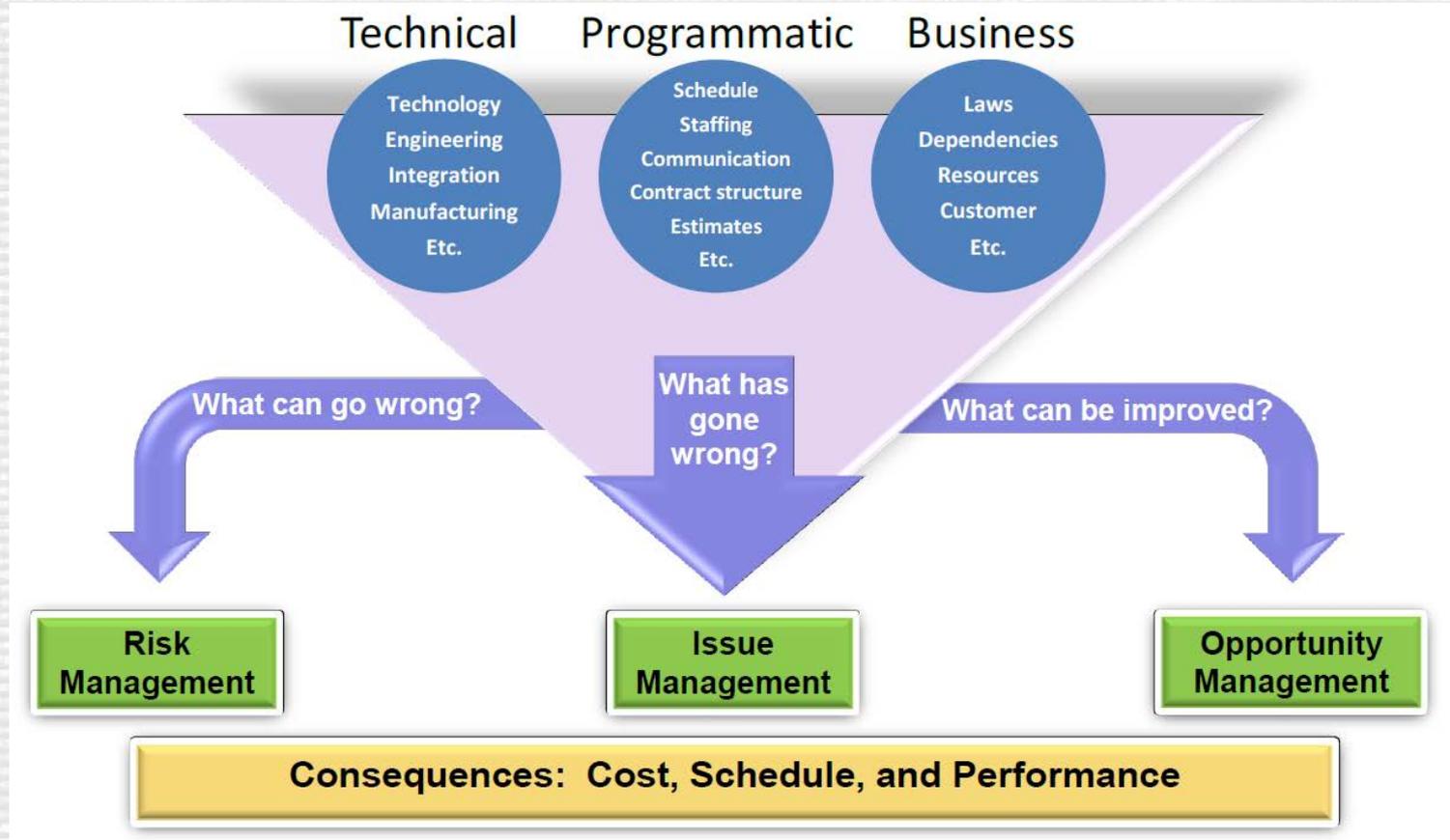
Proactive	Reactive
Preventive	Corrective
Preplanned	Unplanned
Pay Now	Pay More Later
Take Control	Hope for the Best Problem Solving



The goal: Move left and minimize surprises!



RISK, ISSUE, AND OPPORTUNITY RELATIONSHIP



Risk Planning

“Plans are nothing...
planning is everything” DDE



RISK PLANNING



ESTABLISHING AN EFFECTIVE RISK MANAGEMENT PROCESS

Risk management is integral to effective program management. As such, the program should initiate risk management planning and execution as soon as possible in the life cycle. All functional disciplines supporting program planning and execution have a role in risk management.



FRAMING ASSUMPTIONS AND GROUND RULES

Framing Assumptions

priority of requirements

schedule dependencies

accuracy of models and simulations

Ground Rules

Time frame - risk consequence evaluated as if the risk were to be realized without further mitigation, avoidance, etc.

Time of risk event - when risk hypothetically will occur

WBS level - should be ID'd to lowest level possible



ALIGNING GOVERNMENT AND CONTRACTOR RISK MANAGEMENT

Government PMO, Prime Contractor and associated Subcontractors should employ a consistent Risk Management Process

Establish a Joint Risk Management Database

Risk Management should be integrated with:

- Requirements Development;
- Design, Integration, and Test (Systems Engineering);
- Planning and Management of System Support and Sustainment;
- Schedule Tracking;
- Performance measurement;
- Earned Value Management (EVM) (when implemented);
- Cost Estimating;
- Issue Management; etc...



DOCUMENTING THE RISK MANAGEMENT APPROACH

Acquisition Strategy addresses Risk at general level.

Government Systems Engineering Plan (SEP) and the contractor Systems Engineering Management Plan (SEMP) should describe:

- The process for how the program plans to manage risks
- How the risk management processes are integrated with the contractor(s) processes
- How the program identifies and analyzes risks
- How the program plans for, implements (including funding), and tracks risk control
- Key roles and responsibilities from working groups, through the IPT structure up to the executive level
- RMB, who chairs, membership, and meeting frequency
- Risk tool(s) that the program office and contractor use to perform risk management



RISK MANAGEMENT PLAN (RMP)

DoD RIOMG, June 2015

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



RISK MANAGEMENT PLAN (RMP) OUTLINE in DoD RIOMG, June 2015

RISK MANAGEMENT PLAN

- **Introduction** – Overview of the purpose and objective of the RMP.
- **Program Summary** – Brief description of the program, including the connection among the Acquisition Strategy, Program Management Plan, and technical strategy.
- **Definitions** – Definitions specific to the program to be used in the plan.
- **Risk Management Strategy** – Overview of the strategy to implement continuous risk management, to include communication between stakeholders and training of the program team in the risk management process and procedures.
- **Risk Management Board(s) and Risk Working Group(s)** – Description of the formation, leadership, membership, and purpose of these groups.
- **Roles, Responsibilities, and Authorities** – Description of roles, responsibilities, and authorities within the risk management process for:
 - o Identifying, adding, modifying, and reporting risks
 - o Providing resources to handle risks
 - o Developing criteria to determine whether a candidate risk is accepted
 - o Changing likelihood and consequence of a risk
 - o Closing/retiring a risk
- **Risk Management Process and Procedures** – Description of the program risk management process, methodology, meeting battle rhythm, and guidance for implementing the plan, according to the tailorable five-step DoD process:

- o Risk planning
- o Risk identification
- o Risk analysis
- o Risk handling
- o Risk monitoring

- **Risk Management in Relation to Other Program Management**

Tools – List of the risk tools the program (program office and contractor[s]) uses to perform risk management. Preferably, the program office and contractor(s) should use the same tool. If they use different tools, the tools should be capable of seamlessly exchanging data. This section would include a description of how the information would be transferred.

- **Risk Evaluation Techniques** – Summary of the cost, schedule, and performance evaluation processes, including procedures for evaluating risks.

- o Overview and scope of the evaluation process
- o Sources of information
- o Planned frequency of assessments
- o Products and formats
- o Evaluation technique and tools
- o Likelihood and consequence parameters and thresholds

- **Communication and Feedback Process** – Process for communicating and/or elevating the status of potential, current, and retired risks as well as opportunities that may exist to all personnel involved in risk management.



SELECTING A RISK MANAGEMENT TOOL

Risk management tools support the implementation and execution of risk management.

PM needs to select the appropriate risk management tool(s) early and document details in the SEP.

- Support Objectives: Does the tool aid in meeting program objectives?
- Recurrence: Will the risk management tool accommodate recurring updates to the risk management process?
- Helpfulness: Will the tool be useful during the decision-making process?
- Accessibility: Will the tool be accessible to all users, perhaps remotely, including certain tool-licensing requirements?
- Integration: Does the tool aid in the integration with other program management tools and processes?
- Requirements: Does the tool meet the requirements for the program office and contractor(s)?



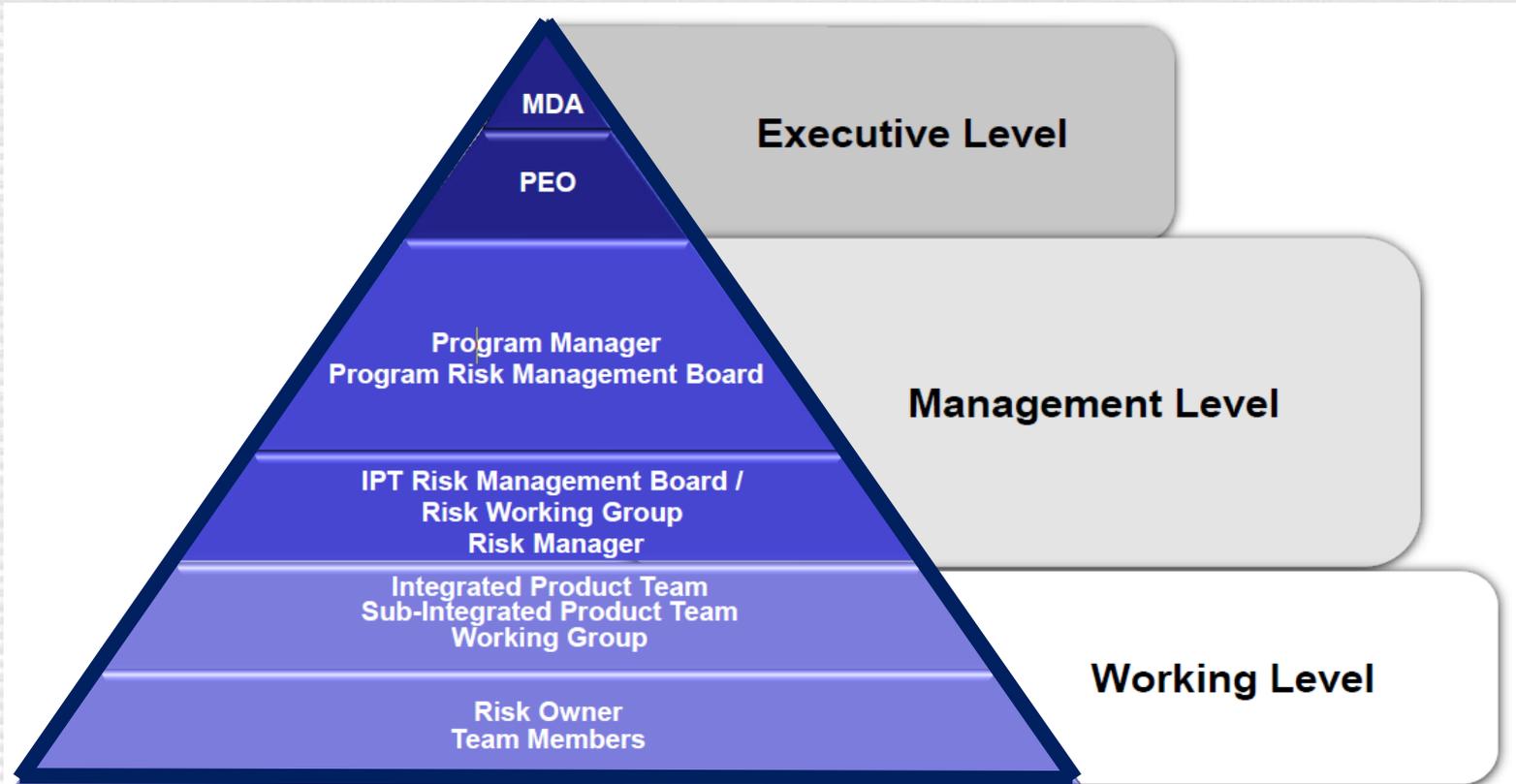
RISK MANAGEMENT BOARD and RISK WORKING GROUP

PM establishes and typically chairs the Risk Management Board (RMB), the approval authority for risk related products

- RMB usually includes PMO functionals e.g. program control, chief engineer, logistics, test, systems engineering, Risk Working Group (RWG) lead, contracting officer, user representative, etc.
- RMB documents actions/decisions in minutes and/or the risk register
- Consider integrated government-contractor RMBs where practical
- Tiered structure is often implemented



ROLES AND RESPONSIBILITIES



Details of Roles and Responsibilities contained in Appendix D of RIOMG



RISK BATTLE RHYTHM

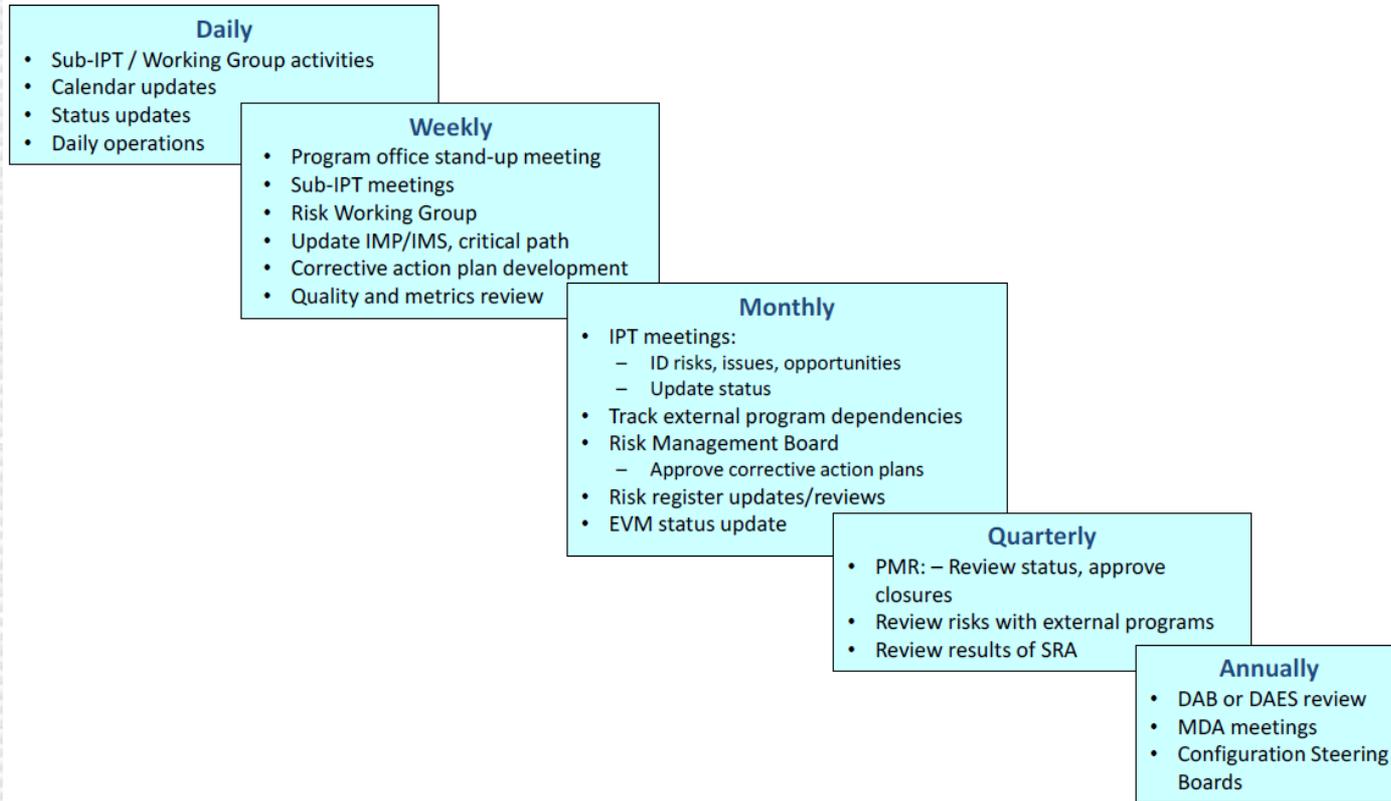


Figure 2-1. Sample Risk Management–Related Battle Rhythm



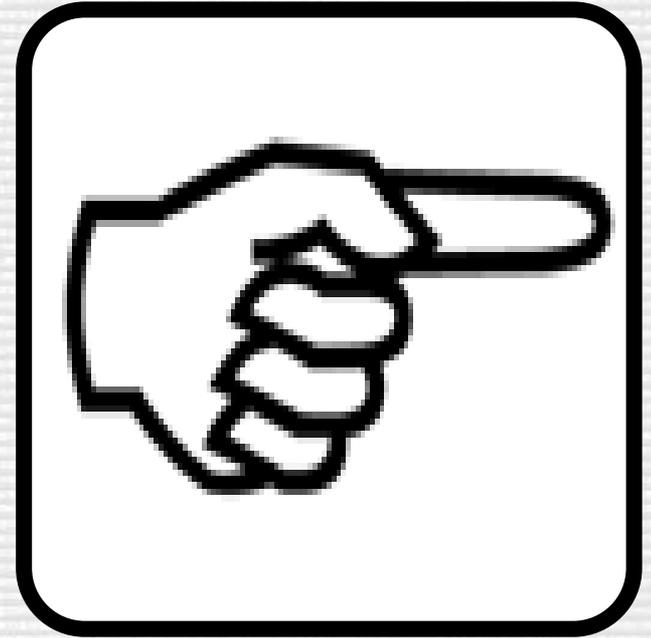
RISK PLANNING SUMMARY

Risk planning consists of the activities to develop, implement, and document the risk management process. Effective planning should outline each of the risk management steps

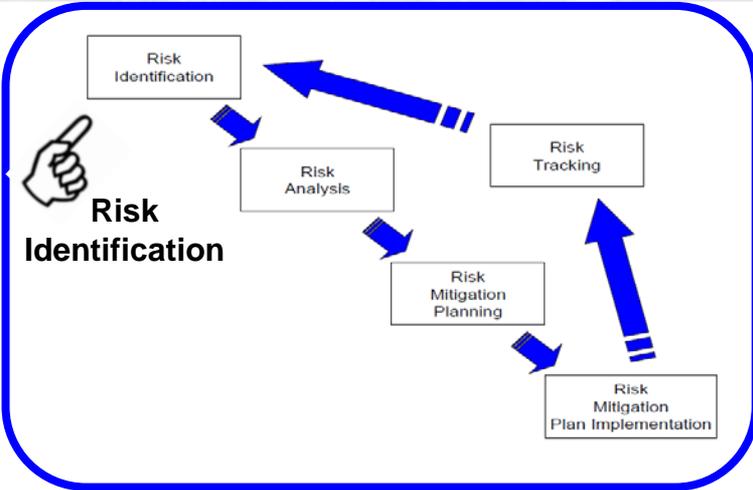
Risk planning should be summarized in the SEP and the RMP and should address the program's risk management organization (e.g., RMBs, frequency of meetings and members), ground rules and assumptions, candidate risk categories, and use of any risk management tools.



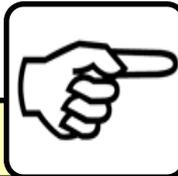
Risk Identification



RISK IDENTIFICATION IN DOD RMG V6 AND DOD RIOMG MODELS



DoD RMG v6 2005



IDENTIFYING RISK: WHAT CAN GO WRONG?



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)**



IDENTIFYING RISK: WHERE TO LOOK FOR POTENTIAL RISKS

Types

- Technical Performance
- Schedule
- Cost

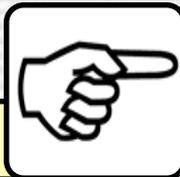
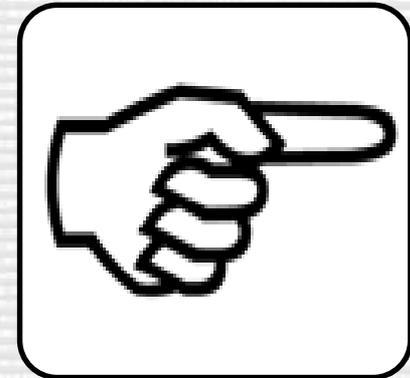
Sources

- Product
- Process
- Scenario

Categories

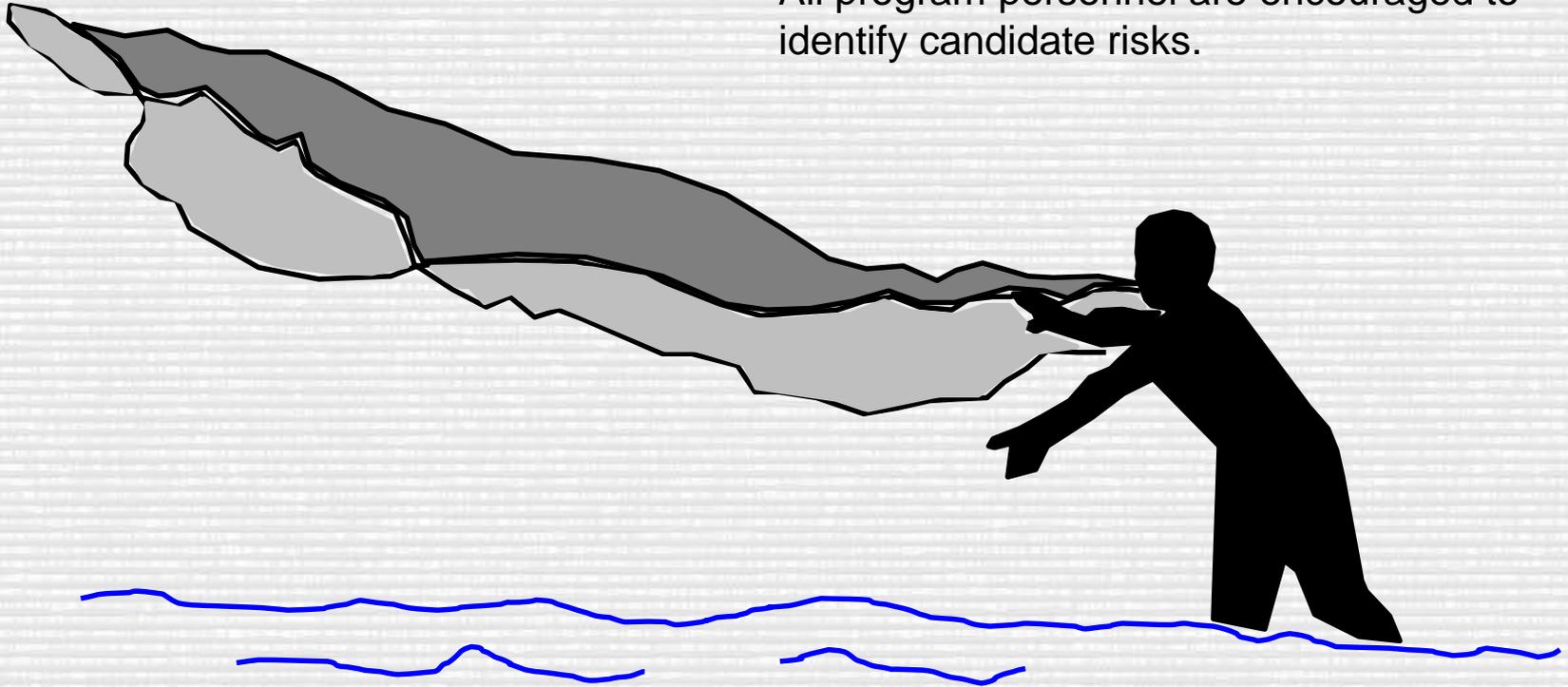
- Technical
- Programmatic
- Business

RISK?



RISK IDENTIFICATION

All program personnel are encouraged to identify candidate risks.



Cast your net wide at first! Do not ignore areas or eliminate ideas early in the process.



TOP-LEVEL RISK ID SOURCES

Where to fish ...



- Analysis of Alternatives (AoA)
- Acquisition Strategy
- Systems Engineering Management Plan (SEMP)
- Test and Evaluation Management Plan (TEMP)
- Technology Readiness Assessment (TRA)
- Program Protection Plan (PPP)
- Life-Cycle Sustainment Plan (LCSP)
- Life-Cycle Mission Data Plan (LMDP)
- Acquisition Program Baseline (APB)
- Systems Engineering Plan (SEP)
- Integrated Master Plan (IMP)
- Integrated Master Schedule (IMS)
- Contract structure and provisions
- Government technical requirements and specifications documents
- Joint Capabilities Integration and Development System (JCIDS) documents



LOWER-LEVEL RISK ID SOURCES

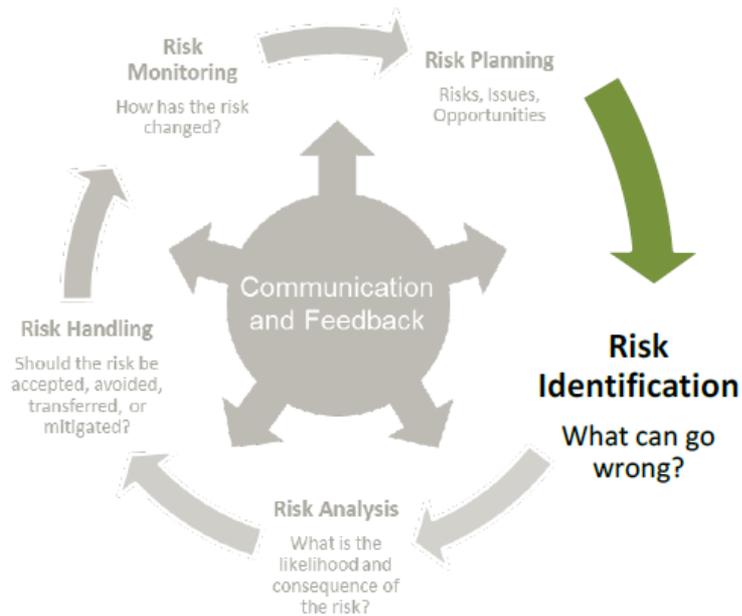
- SME brainstorming activities
- Interviews with program team leads, SMEs, and/or program stakeholders
- Review of lessons learned, including risks or issues on predecessor or similar programs
- Examination of new contract activity and proposals, e.g., the IBR
- Tech Reviews
- Requirements Analysis
- Immature Technologies
- Design Shortfalls
- Trade Studies
- ID of cost/schedule/performance drivers
- Checklists
- Trigger Questions on Key Processes
- Evaluation of results from competitive and risk reduction prototyping
- Evaluation of results from integration and test activities
- Design changes

Where to fish ...

- Leading indicators
- FMEA and other Reliability Analysis
- Specialty engineering e.g. manning, HSI, supportability/sustainment ...
- PPP and Cybersecurity
- Independent Assessments
- Trends in progress toward meeting KPPs, KSAs, TPMs, schedules, budgets, EVM, and other metrics
- External influences:
 - Changes in user requirements, threats, CONOPs, and requirements creep
 - Funding levels
 - Other stakeholder requirements
 - Synchronization with critical external programs
 - Statutory / Service or DoD policy changes
- Production Considerations



WHEN IDENTIFYING RISKS



When identifying risks:

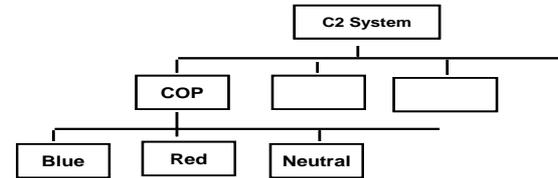
- Example risk ID methodologies:
 - Independent assessments
 - SOW requirements
 - Brainstorming sessions with SMEs
 - Interviews with IPT leads, Systems Command/Center competencies
 - Review of similar/historical programs
 - Trade studies
- Review analysis of Technical Performance Measurements, resource data, life cycle cost information, WBS/IMS/EVM data trends, and progress against critical path
- Review Systems Engineering Technical Review Checklists



3 MORE WAYS FOR RISK ID

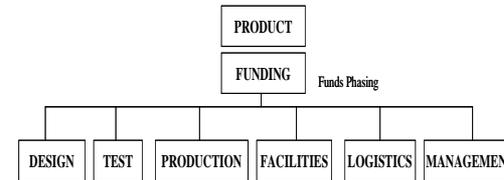
1. Product based evaluation

- Uses Work Breakdown Structure
- Looks at system architecture
- Identifies program relationships



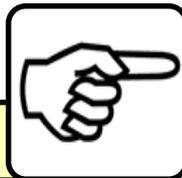
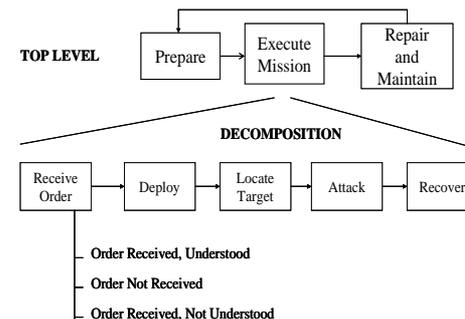
2. Process based evaluation

- Focuses on processes used to define, develop and test a system
- Looks at internal organizational processes



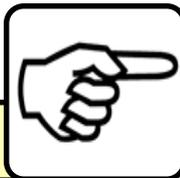
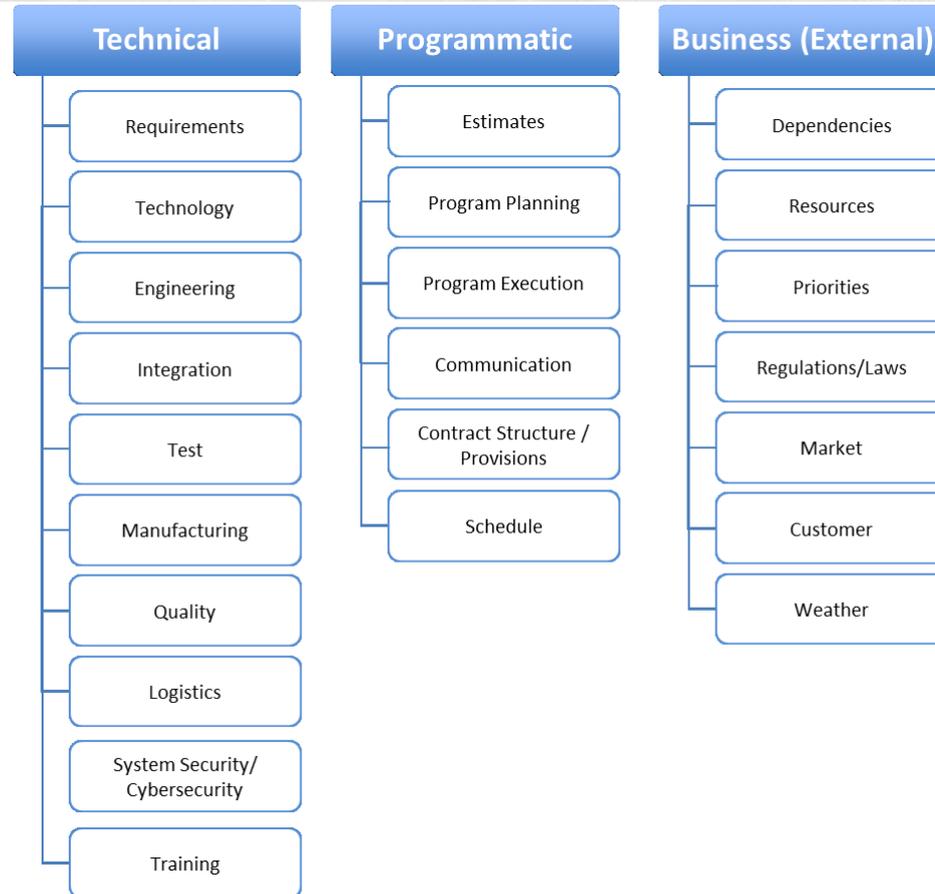
3. Scenario based evaluation

- Risks from a customer and supplier point of view
- Requires knowledge of customers and suppliers, or their inputs/time



RISK CATEGORIES

RISKS can be broadly grouped into three categories:



MORE 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

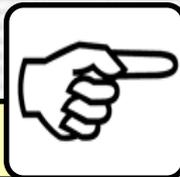
Stability

Developmental Approach

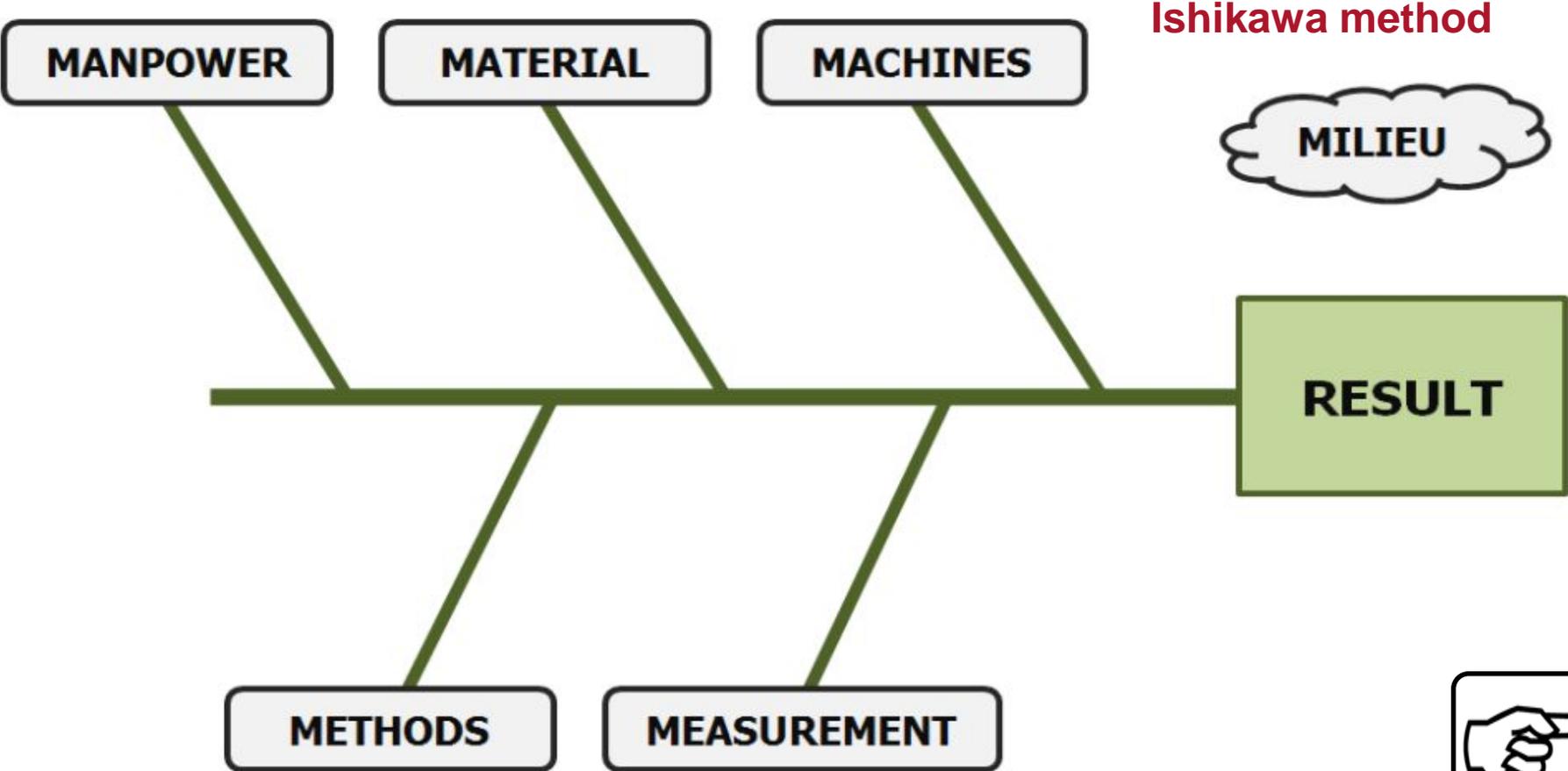
Process Model

Process Maturity

Integration Approach



IDENTIFYING RISK USING THE 5 M'S



EXERCISE: RISK DRIVERS



RISK STATEMENTS

The risk description should be a single declarative statement generally following the format below:



Two examples:

Risk #1: **if** the V1.3 software is not able to provide properly formatted mission data to Program A, **then** Program A may not meet a Key Performance Parameter.

Risk #2: **if** there is a delay in receiving software updates, **then** Program A's production timeline may not be met.



RISK IDENTIFICATION EXAMPLE

If

Some negative event occurs



Stuck in Traffic Jam

Then

Something bad may result



Late for important event



RISK IDENTIFICATION EXAMPLE

If

Some negative event occurs



Fail Exam

Then

Something bad may result



may Not Graduate



RISK IDENTIFICATION EXAMPLE

If

Some negative event occurs



Stock Market Crashes

Then

Something bad may result



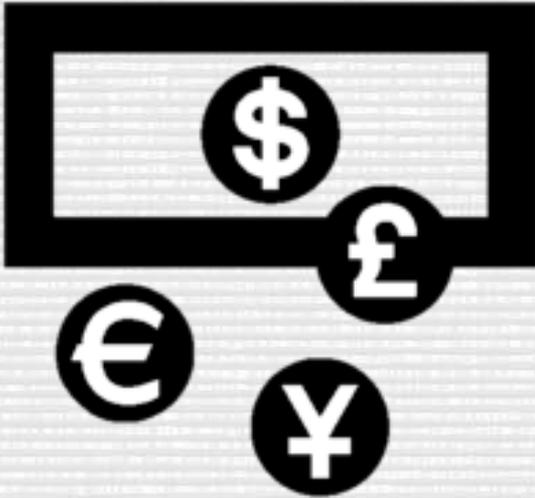
may Not Be Able to Retire



RISK IDENTIFICATION EXAMPLE

If

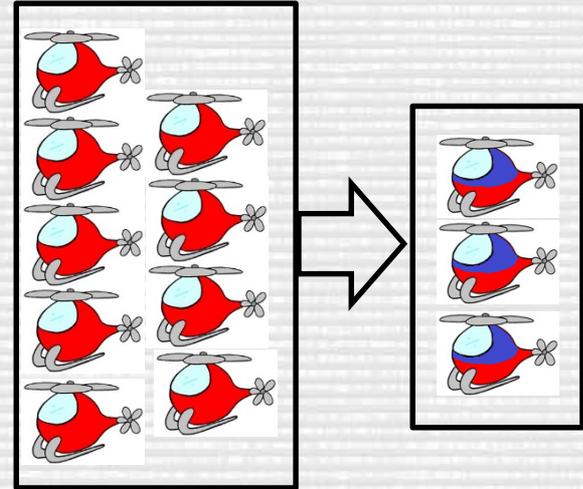
Some negative event occurs



Exchange Rate Changes

Then

Something bad may result



FMS Customer Buys Less



RISK IDENTIFICATION EXAMPLE

If

Some negative event occurs



Crops Fail

Then

Something bad may result



Starve



IF – THEN IS NOT ENOUGH

Good “If – Then” Statements are Critical to effective Risk Management but they are not enough ...



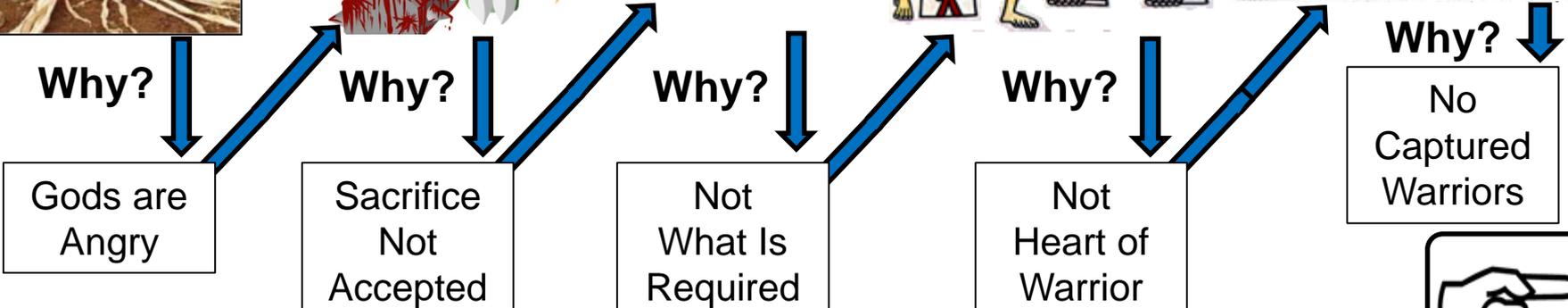
okay... but so what? Must know WHY in order to do something about it (Handling).



ROOT CAUSE DETERMINATION

If
Crops Fail

WHY?



Ask "Why" multiple times until the root cause(s) is (are) discovered



RISK ID AND ROOT CAUSE

Untold numbers sacrificed over at least 1000 years throughout much of Mesoamerica
... but did they correctly identify the risk?



RISK IDENTIFICATION METHOD

Another way to phrase risk statements:

We (the project) might not ...
(deliver some promise)
(meet some expectation)

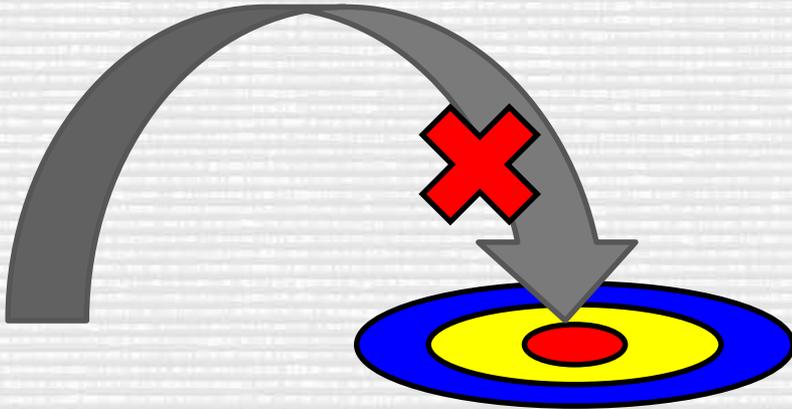
Because ...
(some reason)



RISK IDENTIFICATION EXAMPLE

We might not

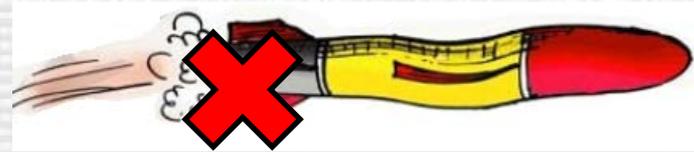
Some promise



Meet Required Mission Range

Because

Some reason



Engine Died



RISK IDENTIFICATION EXAMPLE

We might not

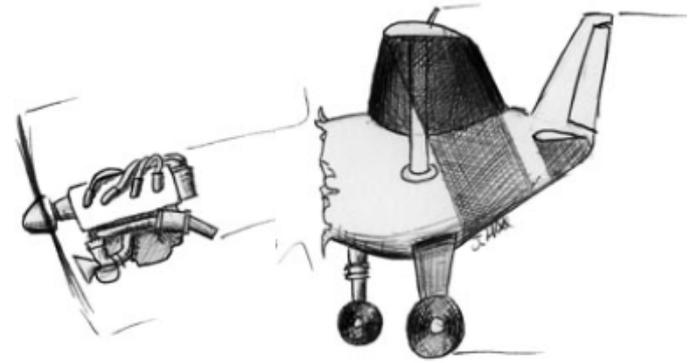
Some promise



Meet Delivery Schedule

Because

Some reason



Acceptance Test Failure



RISK IDENTIFICATION EXAMPLE

We might not

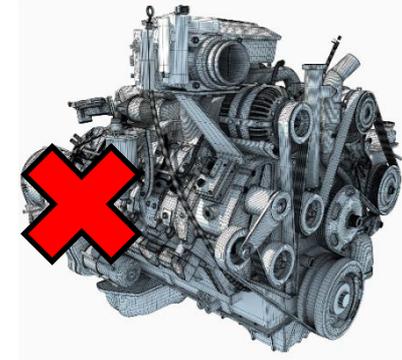
Some promise



Meet Availability Requirements

Because

Some reason



Engine Does Not Start



RISK IDENTIFICATION

MUST DRILL DOWN

The project might not:

(deliver some promise)

(meet some expectation)

Because:

(some reason)

(some reason)

(some reason)

(some reason)

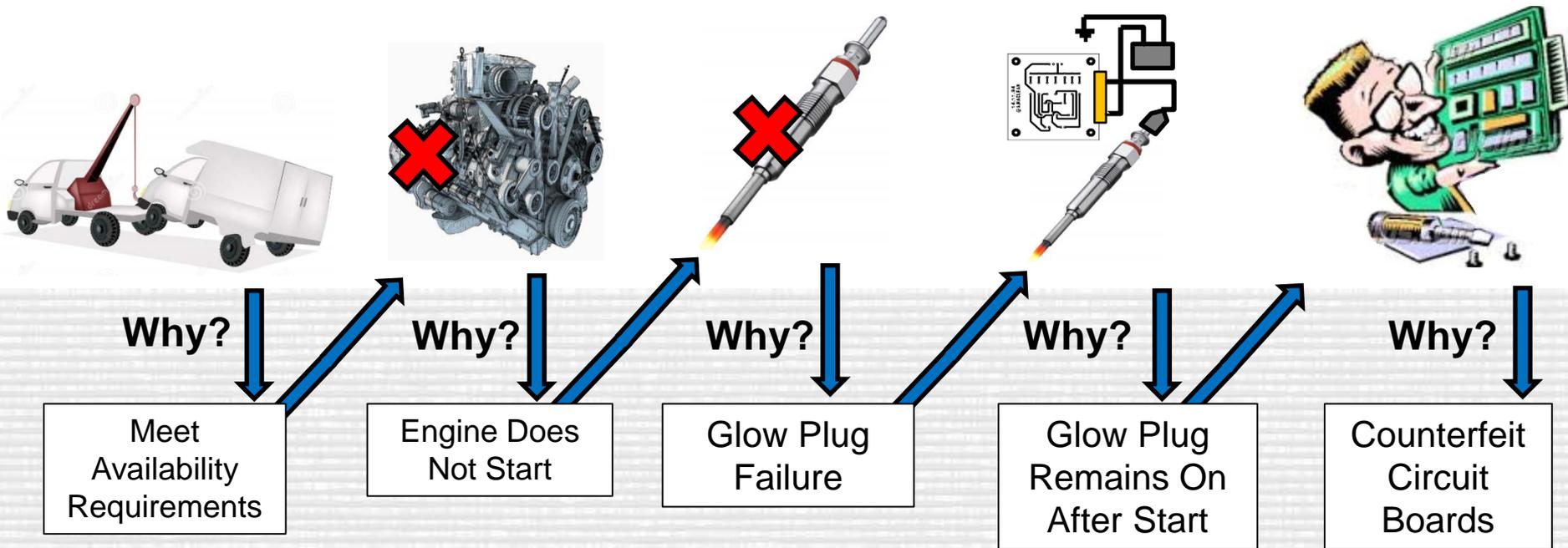
(some fundamental reason)



ROOT CAUSE DETERMINATION

We Might Not:

Because:



Ask "Why" multiple times until the root cause(s) is (are) discovered



ROOT RISK EVENT

If

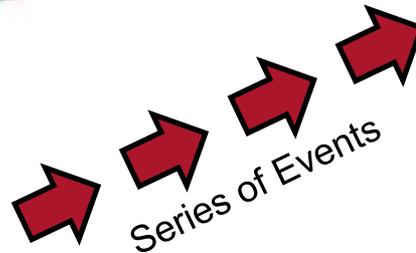
Some negative event occurs

Then

Something bad may result



Purchase Counterfeit
Circuit Boards



Fail to Meet
Availability
Requirements

"Root Risk Event"

"Consequence"



RISK IDENTIFICATION METHOD

Yet another way to phrase risk statements:

There is a probability that...

some (risk event AKA root cause) may occur...

Resulting in... (some negative outcome)

may also add:

Because... (some reason)



WEAK RISK STATEMENTS

Makes an overly general observation:

- **Weak:** *If the high vacancy rate in engineering staff persists, then the program staffing will be inadequate.*
- **Stronger:** *If the high vacancy rate in software engineering staff persists due to aggressive recruiting by competitors, then the commitment to deliver first software builds in 6 months will not be met.*

Identifies an issue rather than a risk:

- **Weak:** *Fatigue cracks discovered in already produced vehicles may shorten service life unless remedied.*

Diverts focus from the program's controllable activities:

- **Weak:** *If the program's funding is withheld due to poor test results, then the program schedule will be jeopardized.*
- **Stronger:** *If the vehicle reliability test performance is below XX MTBF during test, then the resulting schedule delay to fix failures could jeopardize FY 2018 funding.*



EXERCISE: RISK STATEMENTS

Formats:

- a) IF (some event) THEN (some consequence)
- b) WE MIGHT NOT (some promise) BECAUSE (some reason)
- c) THERE IS A PROBABILITY THAT (some risk event) MAY OCCUR,
RESULTING IN (some negative outcome),

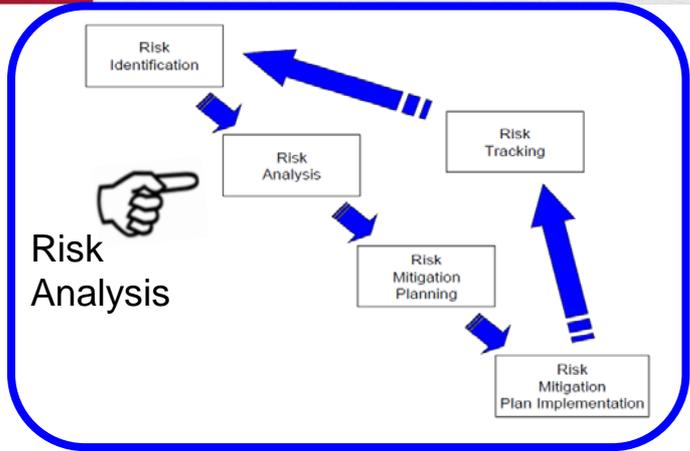
(optional) BECAUSE (some reason)



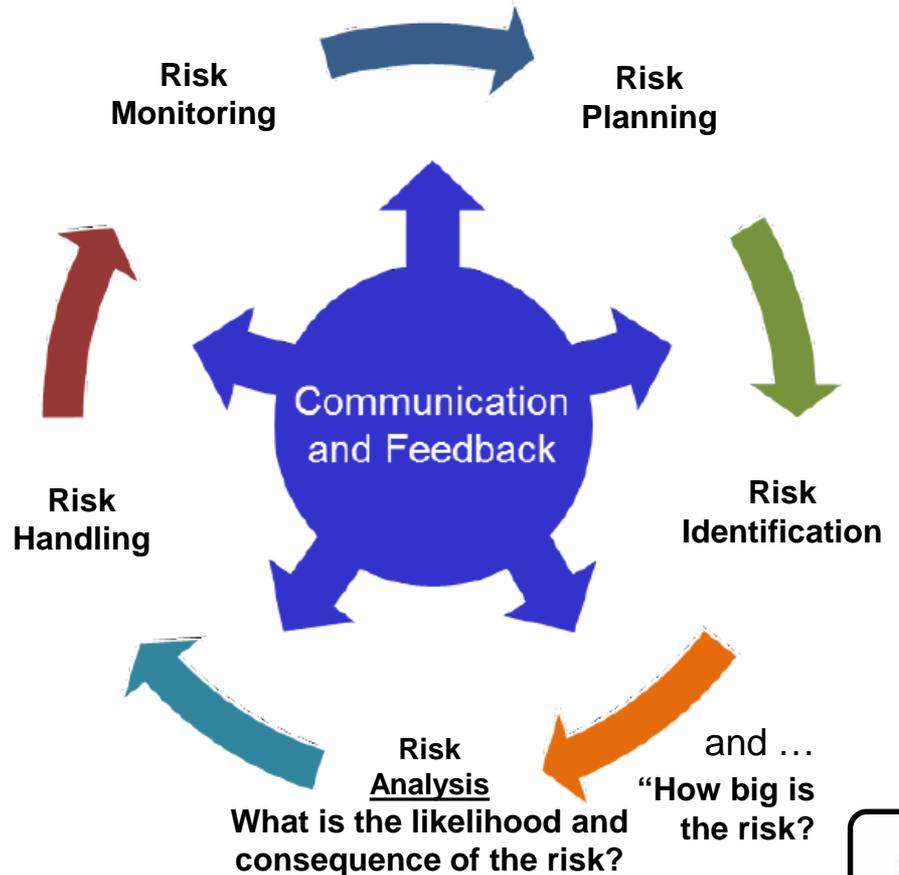
Risk Analysis



RISK ANALYSIS



DoD RMG v6 2005



ANALYZING RISK: WHAT DO RISKS MEAN?

Estimate Likelihood/Consequence

- Technical Performance
- Schedule
- Cost

Determine the Risk Level

- Use consistent predefined likelihood and consequence criteria

Government and Contractor should use common framework

Use Quantitative Data when possible



ANALYZING RISK: HOW BIG IS THE RISK?

Answers the question:

“How big is the risk?”

Iterative process that examines the cost, schedule, and performance parameters of risks

Determines risk likelihood and consequence to achieving program objectives

Examine each identified risk to:

- refine the description of the risk
- isolate the cause
- determine the effects to aid in risk mitigation



ANALYZING RISK: LIKELIHOOD AND CONSEQUENCE?

Also answers the question “*What is the likelihood and consequence of the risk?*”

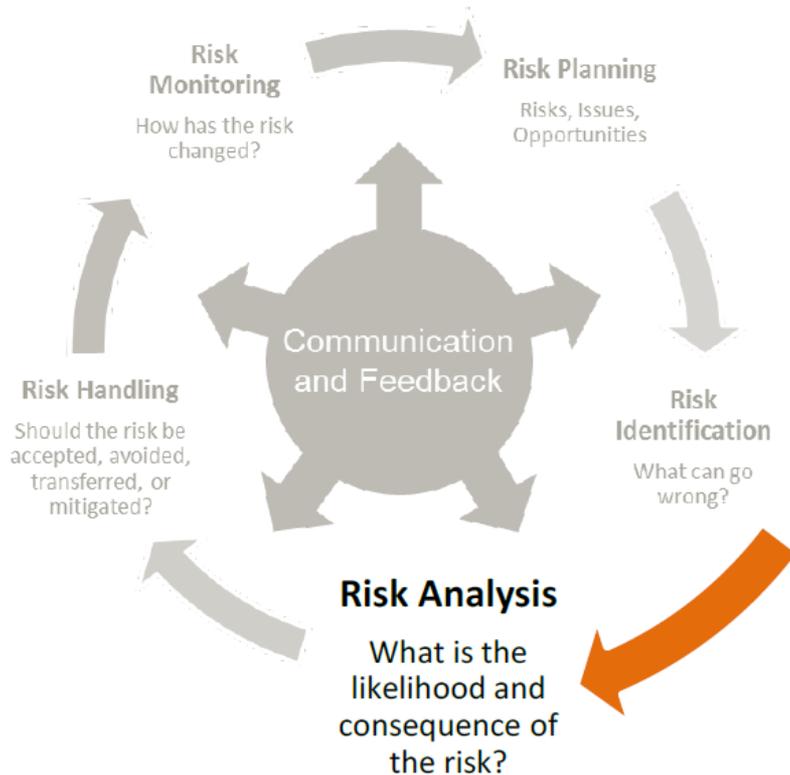
Considering the likelihood the risk event will occur

Identifying the possible consequences in terms of performance, schedule, and costs

Identifying the risk level in the risk reporting matrix



ANALYZING RISK:



When analyzing risks:

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



RISK ANALYSIS CRITERIA

- When analyzing risks, each risk should be evaluated in terms of impact to the program (i.e., effect of the event on program cost, schedule, and performance) should the risk be fully realized.
- Risk consequence is measured as a deviation against program cost, schedule, and performance baselines.
- While the government and contractor will at times have different perspectives on risks and priorities, they should seek to have a common framework for risk consequence and likelihood criteria.



CONSEQUENCE CRITERIA

Levels and Types of Consequence Criteria

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. Slip < <u> </u> month(s)	Budget increase or unit production cost increases. < ** (1% of Budget)
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. Slip < <u> </u> month(s) Sub-system slip > <u> </u> month(s) plus available float.	Budget increase or unit production cost increase < ** (5% of Budget)
4	Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success	Program critical path affected. Slip < <u> </u> months	Budget increase or unit production cost increase < ** (10% of Budget)
5	Severe degradation in technical performance; Cannot meet KPP or key technical/supportability threshold; will jeopardize program success	Cannot meet key program milestones. Slip > <u> </u> months	Exceeds APB threshold > ** (10% of Budget)

Tailored to program



CONSEQUENCE CRITERIA

Level	Cost*			Schedule	Performance
	RDT&E	Procurement	Operations & Maintenance/Sustainment		
5	Major impact. 10% or greater increase over APB threshold; or >\$D. Management reserve depleted.	Major impact. Budget or unit production cost (e.g., APUC) increasing to a significant Nunn-McCurdy breach; or increase of more than \$XX in programmed dollars (POM)	Costs exceed life cycle ownership cost by 10%.. Ability to sustain system in jeopardy.	Schedule slip that requires a major schedule re-baselining; precludes program from meeting its APB schedule objectives by more than 6 months; negative float to program completion	Severe degradation precludes system from meeting a KPP or key technical/supportability threshold; will jeopardize program success; design or supportability margins exceeded; unable to meet mission objectives (defined in mission threads, ConOps, OMS/MP)
4	Significant impact. 5% -<10% increase over APB threshold; or \$C-≤\$D. Requires use of significant management reserves.	Significant impact. Costs that drive a unit production cost (e.g., APUC) increasing to an APB threshold breach of \$C - ≤ \$D; or increase of \$YY-XX in programmed dollars (POM)	Costs drive increase of more than z% over program's lifecycle cost estimate; costs drive program to exceed life cycle ownership cost KSA.	Significantly impacts ability to meet planned milestones and/or other key dates. Established acquisition decision points or milestones will be delayed, impacting APB schedule objectives by less than 6 months. Slip puts funding at risk; <5% float to major milestones or program completion	Significant degradation impairs ability to meet a KSA; Technical design or supportability margin exhausted in key areas; able to meet one or more mission tasks . (defined in mission threads, ConOps, OMS/MP); workarounds required to meet mission objectives
3	Moderate impact. 3% -<5% increase over APB threshold; or \$B - ≤ \$C; manageable with reserves; inability to meet key cost metrics	Moderate impact. Costs that drive unit production cost (e.g., APUC) increase of \$B - ≤ \$C; or \$ZZ-YY in programmed dollars (POM); inability to meet key cost metrics	Costs drive increase of y - z% over program's lifecycle cost estimate or within 2% of life cycle ownership cost KSA; inability to meet key cost metrics	Minor schedule slip, able to meet key milestones. Total program float decreased by X-Y% with float remaining positive, but nearly consumed; <10% float to major milestones or program completion; inability to meet key schedule metrics	Moderate reduction in technical performance or supportability, unable to meet lower tier attributes (e.g. PAs); planned design or supportability margins reduced; inability to meet key TPMs, CTPs; . Workarounds required to achieve mission tasks (defined in mission threads, ConOps, OMS/MP)
2	Minor impact. 1% - <3% increase over APB threshold; or \$A- ≤ \$B; exceeding cost metrics tripwires	Minor impact. Costs that drive unit production cost (e.g., APUC) increase of \$A- ≤ \$B; or \$AA-ZZ in programmed dollars (POM); exceeding cost metrics tripwires	Costs drive increase of x- y% over program's lifecycle cost estimate; exceeding cost metrics tripwires	Able to meet key dates. Total program float decreased by less than X%, with 10% or greater positive float remaining.; exceeding schedule metrics tripwires	Minor reduction in technical performance or supportability; can be tolerated with little or no impact on program objectives. Design margins will be reduced, but within limits / tradespace; exceeding key TPMs, CTPs tripwires
1	Minimal impact. <1% increase over APB threshold; or <\$A. Costs expected to meet approved funding levels, not projected to increase above thresholds	Minimal impact. Costs that drive APUC increase of ≤ \$A ; or less than \$AA in programmed dollars (POM). Costs expected to meet approved funding levels, not projected to increase above thresholds	Costs drive increase of ≤ \$x% over program's lifecycle cost estimate.	Minimal or no schedule impact.	Minimal or no consequences to meeting technical performance or supportability requirements. Design margins will be met; margin to planned tripwires.

Tailored to program - Programs can break out cost or consolidate

DoD Risk, Issue, and Opportunity Management Guide June 2015



LIKELIHOOD CRITERIA

Levels and Types of Likelihood Criteria

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

Tailored to program



LIKELIHOOD CRITERIA

Table 3-2. Recommended Likelihood Criteria

Level	Likelihood	Probability of Occurrence
5	Near Certainty	> 80% to ≤ 99%
4	Highly Likely	> 60% to ≤ 80%
3	Likely	> 40% to ≤ 60%
2	Low Likelihood	> 20% to ≤ 40%
1	Not Likely	> 1% to ≤ 20%

Specific Criteria Recommended



RISK ANALYSIS

Risks can be characterized as

HIGH, **MODERATE**, or **LOW**

based on predetermined rating thresholds.

Risk Level is calculated for each risk and serves as the means to rank the program risk.

This difficult but important step in the risk management process helps the program determine resource allocation and the appropriate mitigation strategy.



RISK ANALYSIS

How big is the Risk? and
What are the Likelihood and
Consequence should it occur?

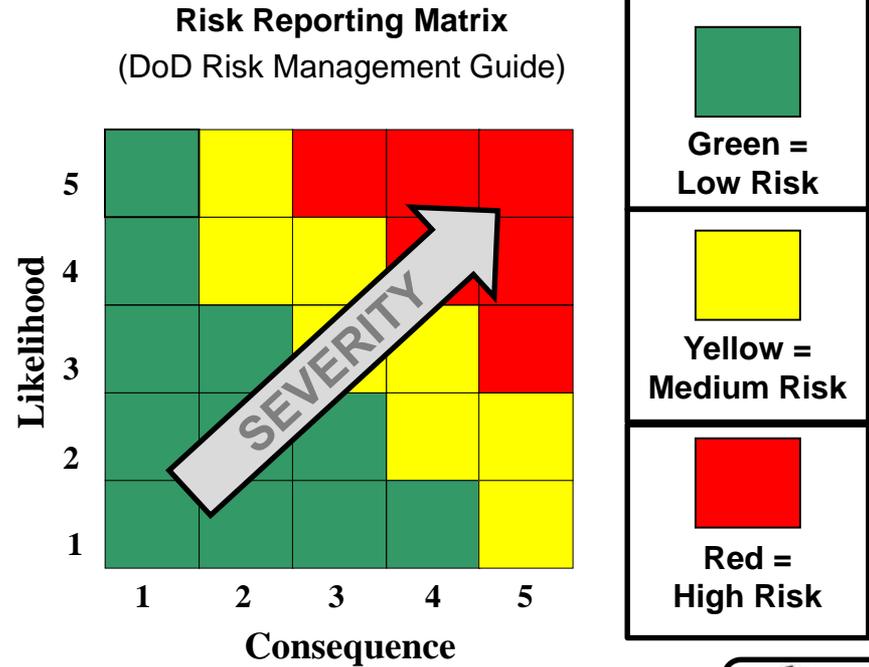
Assess Consequence

Analyze the possible
consequences in terms of
technical, schedule, cost (RDT&E,
Procurement and O&M)

Assess Likelihood of occurrence

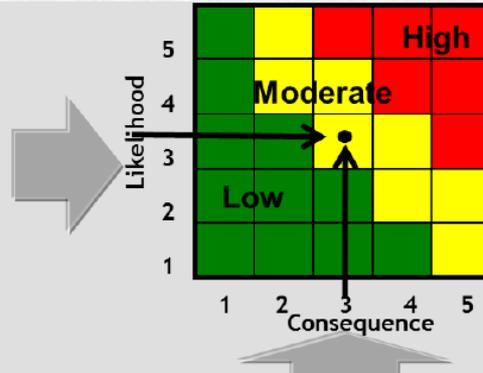
Identify the risk level in the 5X5
risk reporting matrix

Risk Reporting Matrix is the same in
both DoD RMG v6.0 and DoD ROIMG



DOD RISK REPORTING MATRIX

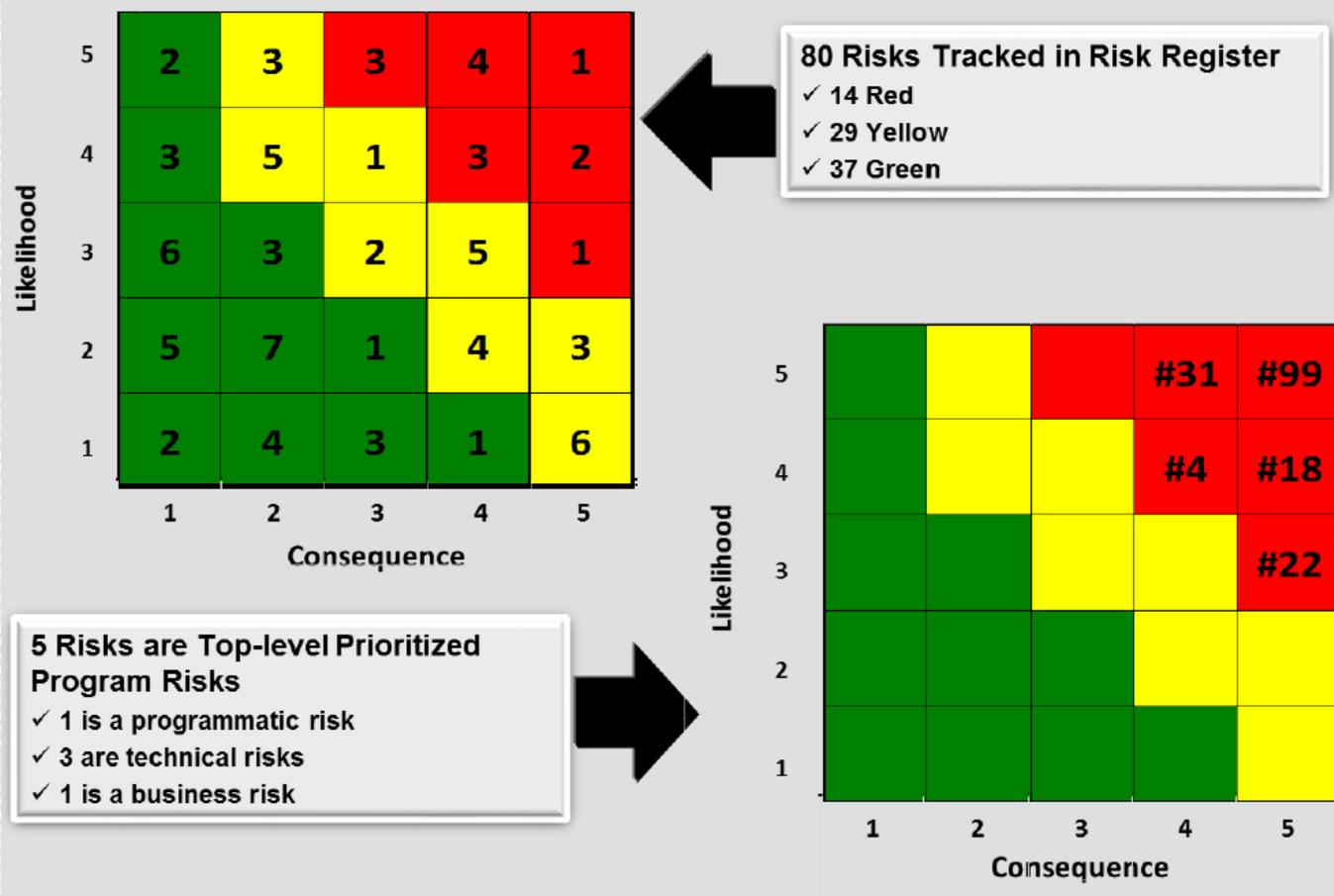
Level	Likelihood	Probability of Occurrence
1	Not Likely	> 1% to ≤ 20%
2	Low Likelihood	> 20% to ≤ 40%
3	Likely	>40% to ≤ 60%
4	Highly Likely	>60% to ≤ 80%
5	Near Certainty	> 80% to ≤ 99%



Level	Cost			Schedule	Performance
	RDT&E	Procurement	Operations & Maintenance		
1	Minimal impact: <1% increase over most recent cost estimate; or, <\$A dollars	Minimal impact: < \$A or < 1% of budget	Minimal or no impact on O&M	Minimal or no impact	Minimal or no consequences to meeting technical performance or supportability requirements Design margins will still be met
2	Minor impact: 1% - <3% increase over most recent cost estimate; or, \$A - ≤ \$B	Minor impact: 1% - <3% increase over unit production cost baseline; or, \$A - ≤ \$B	Increase of x- y% over program's cost estimate	Able to meet key dates. Does not significantly decrease program total float	Minor reduction in technical performance or supportability; can be tolerated with little or no impact on program. Design margins will be reduced, but within acceptable limits
3	Moderate impact: 3% - <5% increase over most recent cost estimate; or, \$B - ≤ \$C; manageable with reserves	Moderate impact: 3% - <5% increase over unit production cost baseline; or, \$B - ≤ \$C; or 1/10 of significant Num-McCurdy (N-M) breach	Increase of y - z% over program's cost estimate	Minor schedule slip. Able to meet key milestones. Significantly decreasing program total float. Impacting the critical path	Moderate reduction in technical performance or supportability with limited impact on program objectives. Design or supportability margins are significantly reduced and jeopardize achieving performance threshold
4	Significant impact: 5% - <10% increase over most recent cost estimate; or \$C - ≤ \$D; Requires use of significant management reserves	Moderate impact: 5% - <8% increase over unit production cost baseline; or, \$C - ≤ \$D; or 1/5 of significant N-M breach	Increase of more than z % over program's cost estimate or within 2% of lifecycle ownership cost KSA	Significantly impacts ability to meet milestone dates and/or other key dates. Significantly impacts ability to meet the program or project completion date. Schedule slip puts funding at risk	Significant degradation in technical performance or major shortfall in supportability; cannot meet a KSA; may jeopardize program success No technical design or supportability margins available
5	Major impact: 10% or greater increase over cost estimate; or >\$D. Program success in jeopardy	Major impact: 8% or more increase over unit production cost baseline; or, >\$D or; 1/2 of a significant N-M breach	Exceeds lifecycle ownership cost KSA. Ability to sustain system in jeopardy	Schedule slip that requires a major schedule re-baselining. Failing to meet milestone dates and/or other key dates; Failing to meet the program or project completion date	Severe degradation in technical performance or supportability; cannot meet KPP or key technical/supportability threshold; Will jeopardize program success



DOD RISK REPORTING MATRIX



EXPECTED MONETARY VALUE

Risk	Likelihood	Consequence Cost	Exposure	Cost to Handle	Return on Investment
Risk 1:	20%	\$10M	\$2M	\$1M	\$1M
Risk 2:	70%	\$10M	\$7M	\$1M	\$6M
Risk 3:	40%	\$36M	\$9M	\$2M	\$7M
Risk 4:	60%	\$5M	\$3M	\$.5M	\$2.5M
Total		\$61M	\$21M	\$4.5M	

Programs should compare cost burdened risk and cost of handling strategies.

Cost exposure of a risk can be expressed as its EMV, which is the likelihood of the risk multiplied by the cost consequence of the risk if realized.

Cost of the risk handling effort is then subtracted from the risk exposure to determine the “likely” return on investment (ROI).



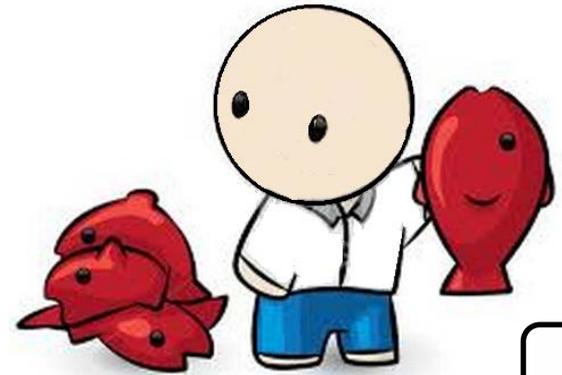
RISK ANALYSIS EXPECTATIONS

➤ ***Expectations:***

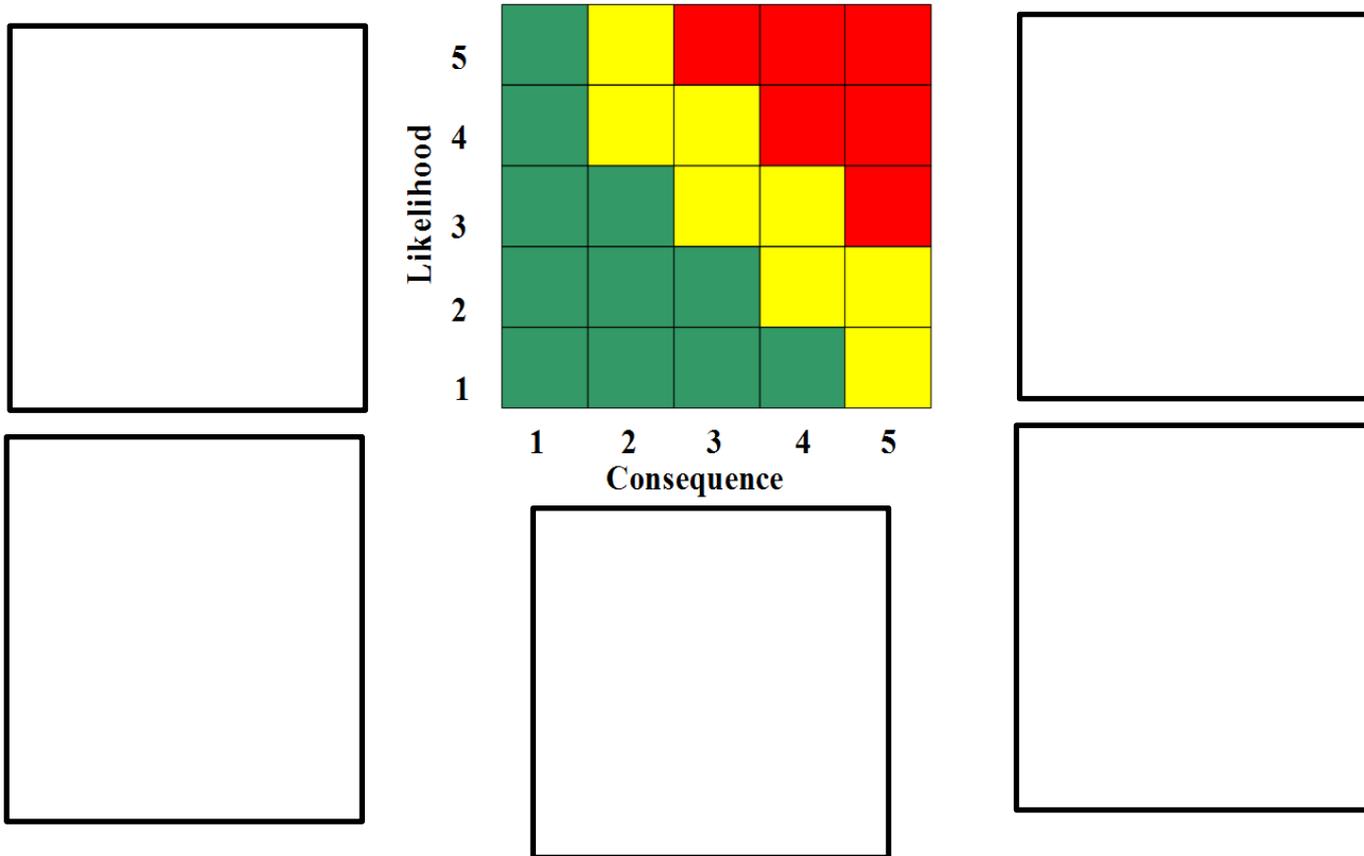
- Risk statements and descriptions fully document events that could adversely affect a program's ability to meet cost, schedule, and performance objectives or baselines.
- Risk statements are clearly written using an “if-then” or similar construct.
- Programs use established criteria, tailored only as necessary, to provide a consistent means for evaluating risks.
- Resulting likelihood and consequence ratings should be supported by data and analysis.
- Programs conduct periodic risk analyses to update risk estimates and to align and support other program activities such as EVM, IMS, and technical reviews.
- If the analyzed likelihood is 100 percent, the program should address the event or condition as an issue rather than a risk.



EXERCISE: RISK ANALYSIS



RISK MATRIX TEMPLATE



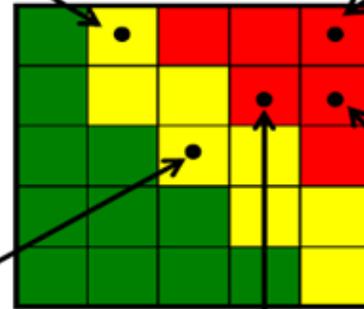
Populate Risk Matrix with Top Five Risks



RISK MATRIX EXAMPLE

- Risk ID Number: 31
- Risk Driver:
- Risk Mitigation Action:
 - Cost: \$
- Closure Date:
- Cost Impacts:
 - RDT&E: \$ or %
 - Production: \$ or %
- Schedule Impacts:
 - Months:
- Performance Impacts:
 - Only achieves XX% of aaa KPP performance

- Risk ID Number: 99
- Risk Driver:
- Risk Mitigation Action:
 - Cost: \$
- Closure Date:
- Cost Impacts:
 - RDT&E: \$ or %
 - Production: \$ or %
 - O&M: \$ or %
- Schedule Impacts:
 - Months:
- Performance Impacts:
 - Only YY% of abc KSA performance



- Risk ID Number: 22
- Risk Driver:
- Risk Mitigation Action:
 - Cost: \$
- Closure Date:
- Cost Impacts:
 - Production: \$ or %
 - O&M: \$ or %
- Schedule Impacts:
 - Months:

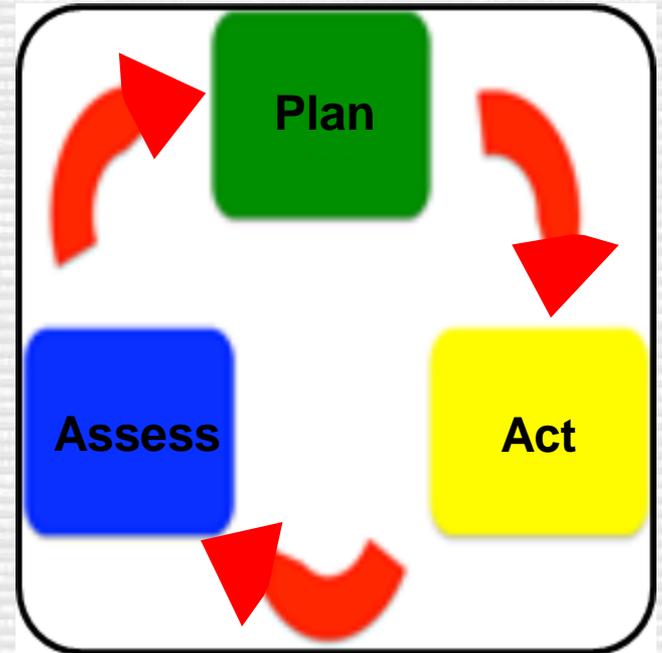
- Risk ID Number: 4
- Risk Driver:
- Risk Mitigation Action:
 - Cost: \$
- Closure Date:
- Cost Impacts:
 - Production: \$ or %
- Schedule Impacts:
 - Months:
- Performance Impacts:
 - May trade xyz performance

- Risk ID Number: 18
- Risk Driver:
- Risk Mitigation Action:
 - Cost: \$
- Closure Date:
- Cost Impacts:
 - RDT&E: \$ or %
 - Production: \$ or %
- Schedule Impacts:
 - Months:

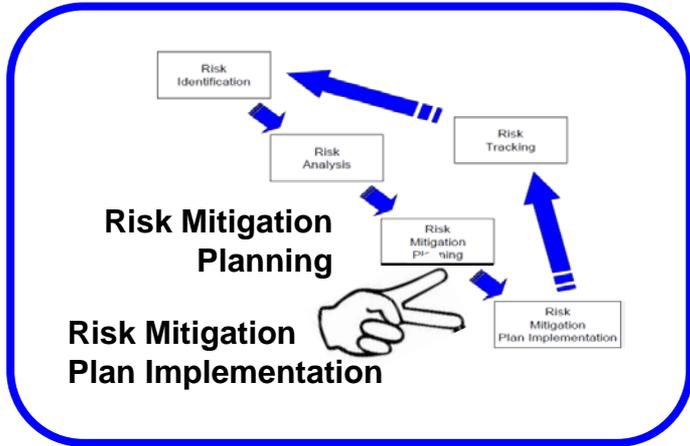


Risk Handling

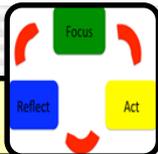
formerly
(Mitigation)



RISK HANDLING

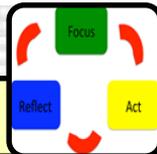


DoD RMG v6 2005



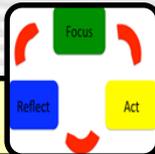
RISK HANDLING

- Consider the accept, avoid, and transfer handling options, not just the mitigation option
- Choose the best handling option, then select the best implementation approach for that option
- Take into consideration elevating the risk to appropriate tiers (executive, management, or working level)
- Include cross-program risks in order to consider the impact of risk management actions on other programs



RISK HANDLING APPROACH

- The selected mitigation approaches for program-level risks should be reflected in the program's Acquisition Strategy
- Include the specifics of **what** should be done,
- **when** it should be accomplished,
- **who** is responsible,
- the **cost** and **schedule** impact, and
- the **funding/resources** required to implement the risk mitigation plan



FOUR FUNDAMENTAL STRATEGIES

Avoid



Eliminate the risk event or condition

Mitigate



Actively reduce risk to an acceptable level

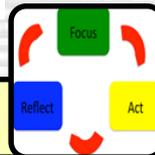
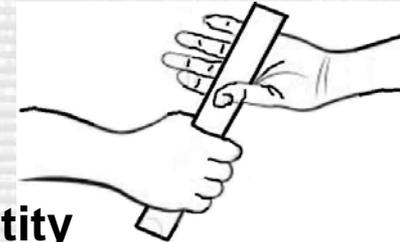
Assume (Accept)



Accept the level of risk, but continuing on the current program plan

Transfer

Transfer to another entity



RISK HANDLING

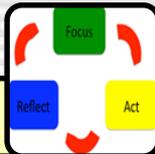
When handling risks:

Consider the accept, mitigate, avoid, and transfer handling options, not just the mitigation option

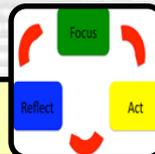
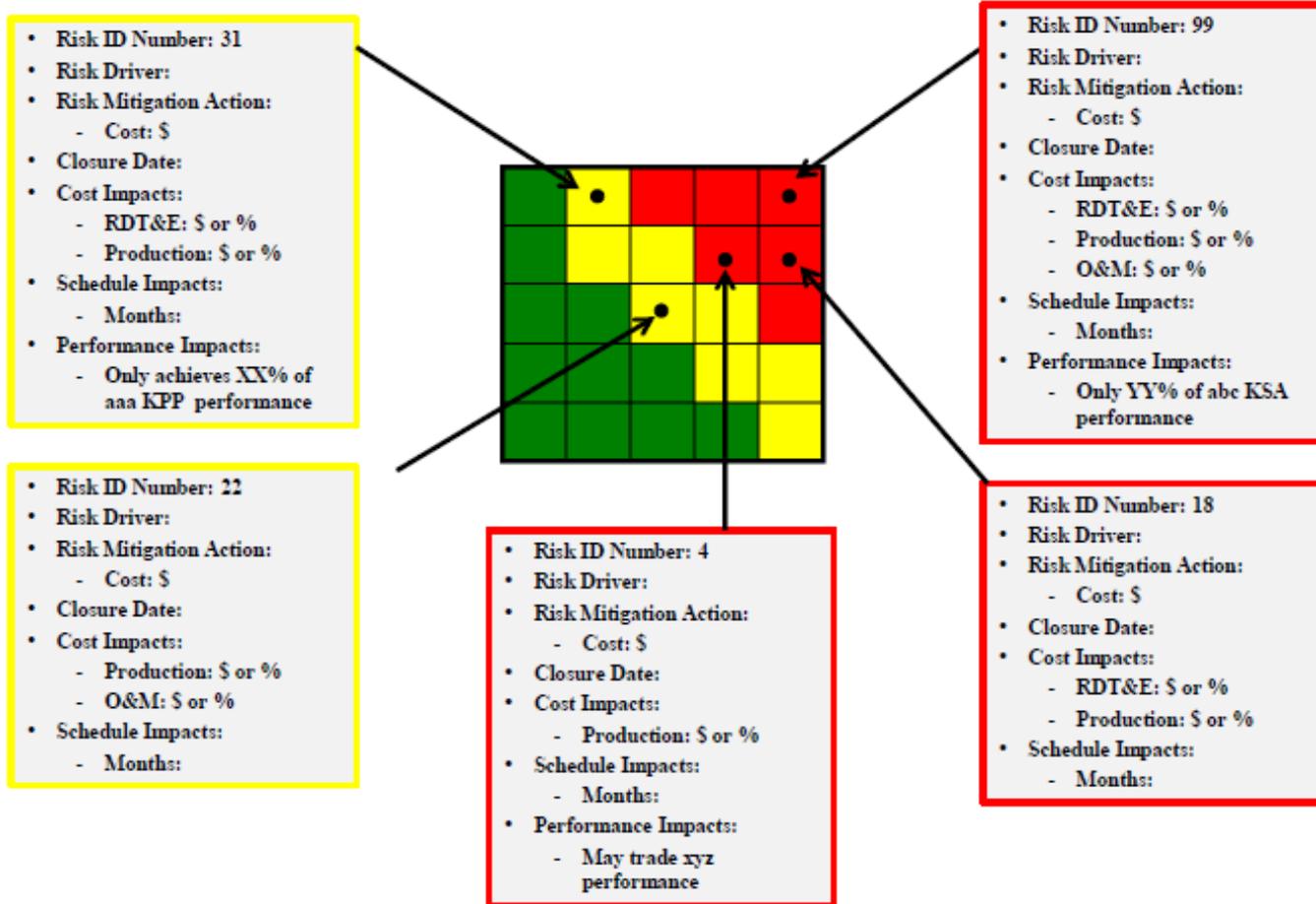
Take into consideration elevating the risk to the appropriate tiers (executive, management or working level)

Include cross-program risks in order to consider the impact of risk management actions on other programs

Tracking the implementation and progress of the risk handling strategy, not just the development and planning of the selected strategy

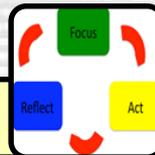


RISK REPORTING MATRIX



RISK REGISTER

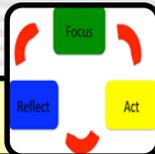
Risk Number	Linked WBS/TMS ID#	Owner	Type of Risk	Status	Tier	Risk Event	Likelihood, Consequence Rating	Risk Handling Strategy	Risk Identified Date	Risk Approval Date	Planned Closure Date	Target Risk Rating	Plan Status
8231	3.2.2	Name	Technical	Open	II	Excessive number of priority 1 and 2 software defects may cause a delay to the start of IOT&E	L=3, C=4	Mitigation - Program will apply management reserve to retain adequate software engineers to burn-down SW defects	8/23/2013	1/14/2014	2/12/2014	L=1, C=4	On schedule



RMB ACTIONS

Risk Management Board (RMB) should compile a list of criteria that answers questions such as:

- Is the approach feasible in implementation?
- Are the expectations realistic in effectively reducing program risk to an acceptable level?
- Is the approach affordable in terms of dollars and resources?
- Is adequate time available to develop and implement the approach?
- What impact do these approaches have on the overall program schedule?
- What impact will the mitigation approach have on the technical performance of the system?



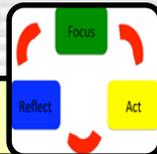
RISK MITIGATION IMPLEMENTATION

RM Implementation

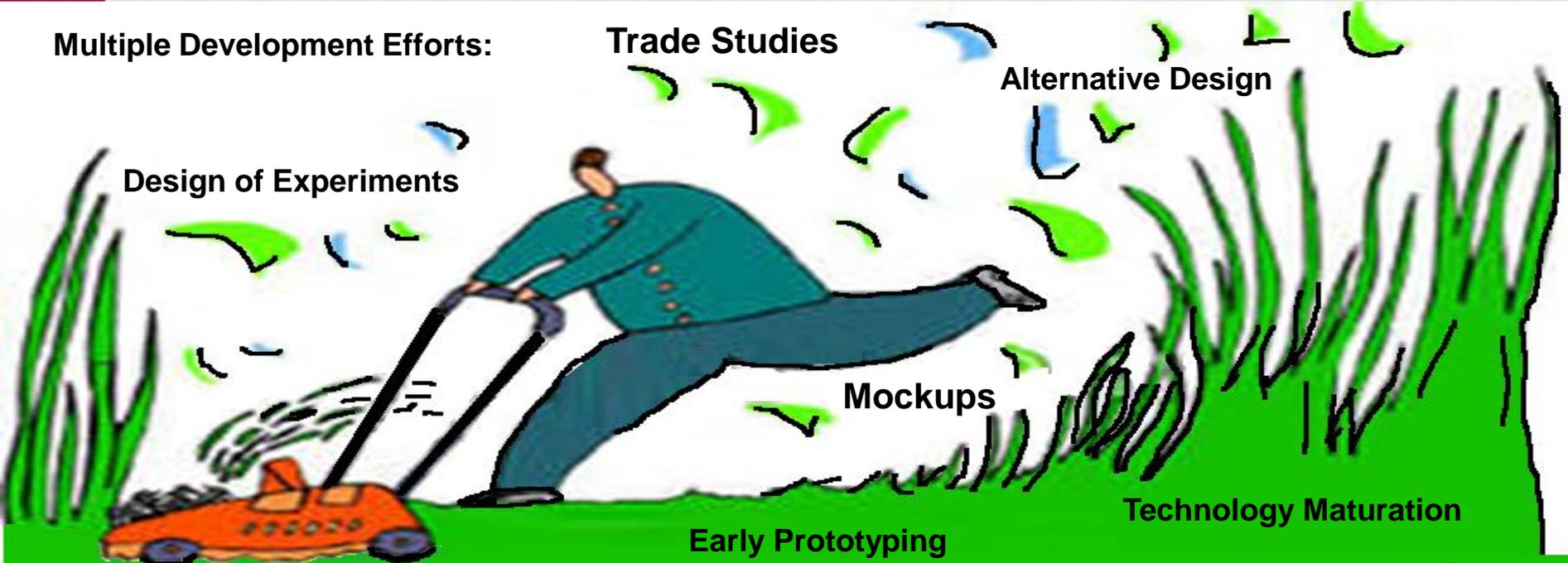
- Directing the teams to execute the defined and approved risk control plans
- Applying resources (manpower, schedule, budget) to reduce the likelihood and/or consequence of risks
- Tracking resource expenditure, technical progress, and risk impacts (benefits)

Reduces Program Risks

- Providing a coordination vehicle with management and other stakeholders
- Outlining the risk reporting requirements for ongoing monitoring, to include “trip wires” which warrant elevating the risk to the next management level
- Documenting the change history
- Providing information to further enhance risk tracking and risk communication



RISK MITIGATION APPROACHES



Multiple Development Efforts:

Trade Studies

Alternative Design

Design of Experiments

Mockups

Early Prototyping

Technology Maturation

Process Proofing

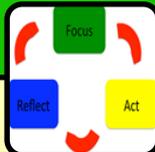
Ways to Mow Down Risk

Robust Design

Demonstration Events

Models and Simulation

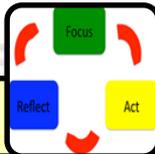
Reviews, Walk-throughs, and Inspections



RISK BURN-DOWN

Burn-down plan consists of 6 steps, tied to the project schedule, that allow the program to control and retire risks

1. Identify risk start and end points on a graph
2. Assign numerical values to these points
3. Identify activities that will burn-down risk
4. Estimate the time basis for these activities
5. Estimate their relative risk burn-down contribution
6. Chart the relationship of activities on a date basis



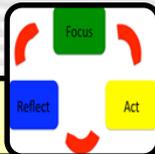
MORE BURN DOWN CONSIDERATIONS

Ensure all risk handling activities

- (1) are clearly defined and jargon free,
- (2) are objective and not subjective, and
- (3) have specific, measurable outcomes. For example, the statement

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

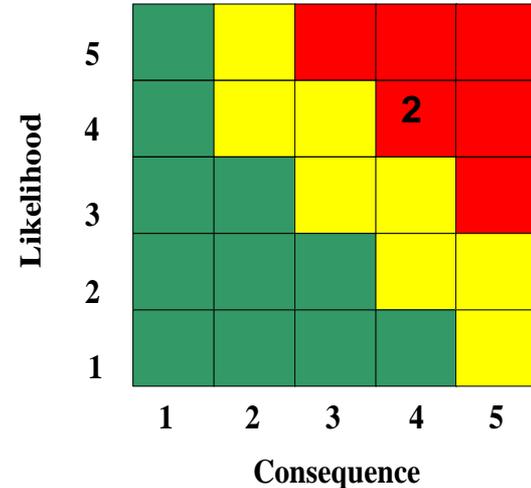
- Not all handling activities will result in a score change or burn-down of the risk but are necessary to track the progress of the burn-down plan (e.g., meetings do not mitigate risks, results do).



RISK MITIGATION PLAN EXAMPLE

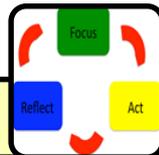
Identify, evaluate, and select detailed steps that will drive risk to an acceptable level given program constraints and objectives

1. Get new/detailed Program A and SW schedules
2. Identify insertion points for SW updates
3. Work with SW contractor to improve schedule
4. Incentivize SW lab construction for schedule
5. Identify root cause of SW technical issues
6. Correct SW technical issues
7. Improve SW schedule by 2 months
8. Improve SW lab construction by 1 month
9. New SW dates coordinated with Program A leadership



EXAMPLE

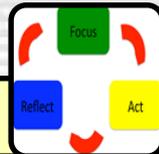
Risk #2: If the timeline established for Program A's production is not met because of a delay in receiving software updates, then there will be a program slip of at least 4 months.



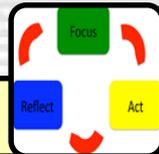
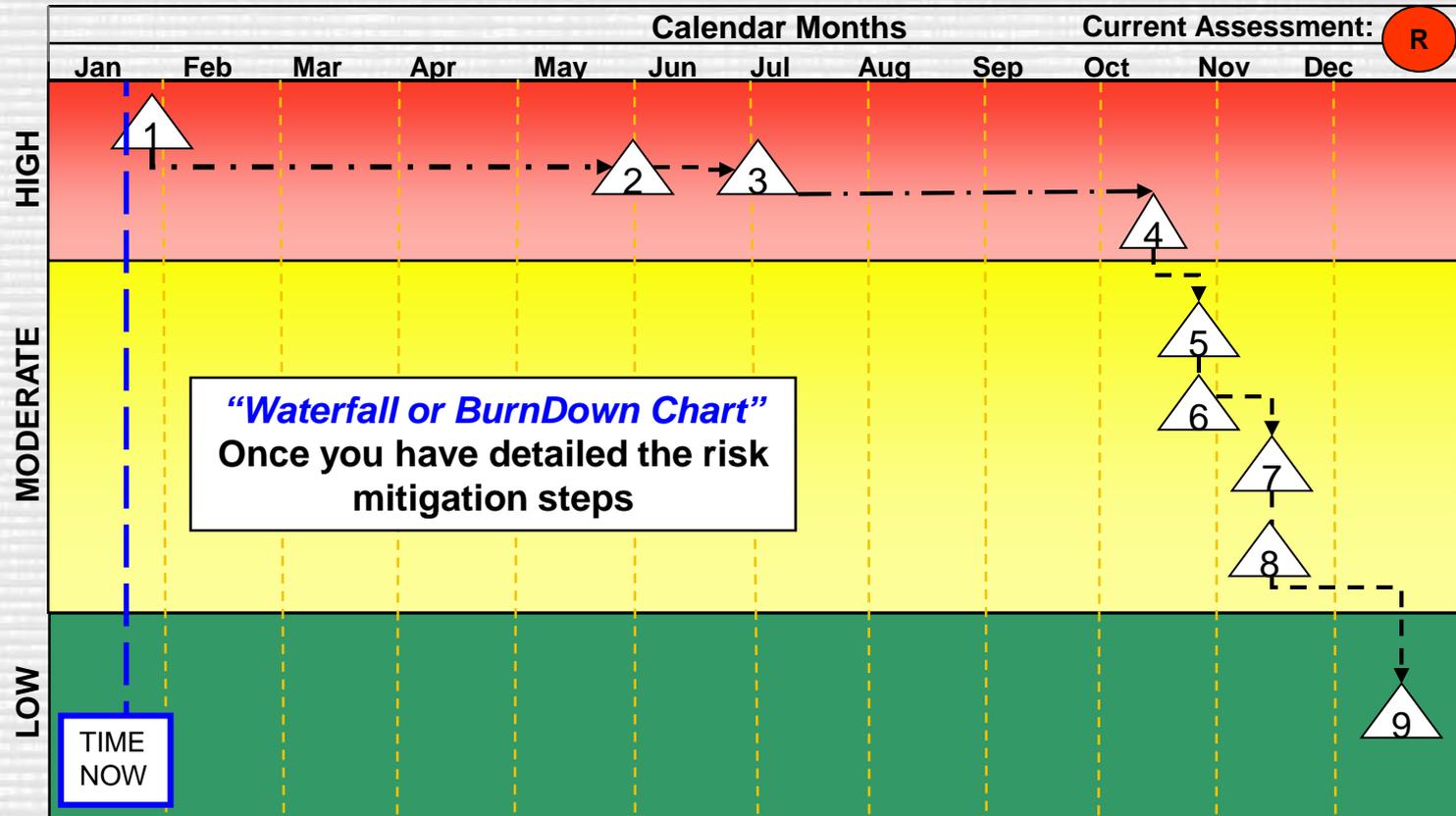
RISK MITIGATION PLAN EXAMPLE

Include the specifics of what should be done, [when](#) it should be accomplished, [who](#) is responsible, and [funding](#) required to implement mitigation strategy

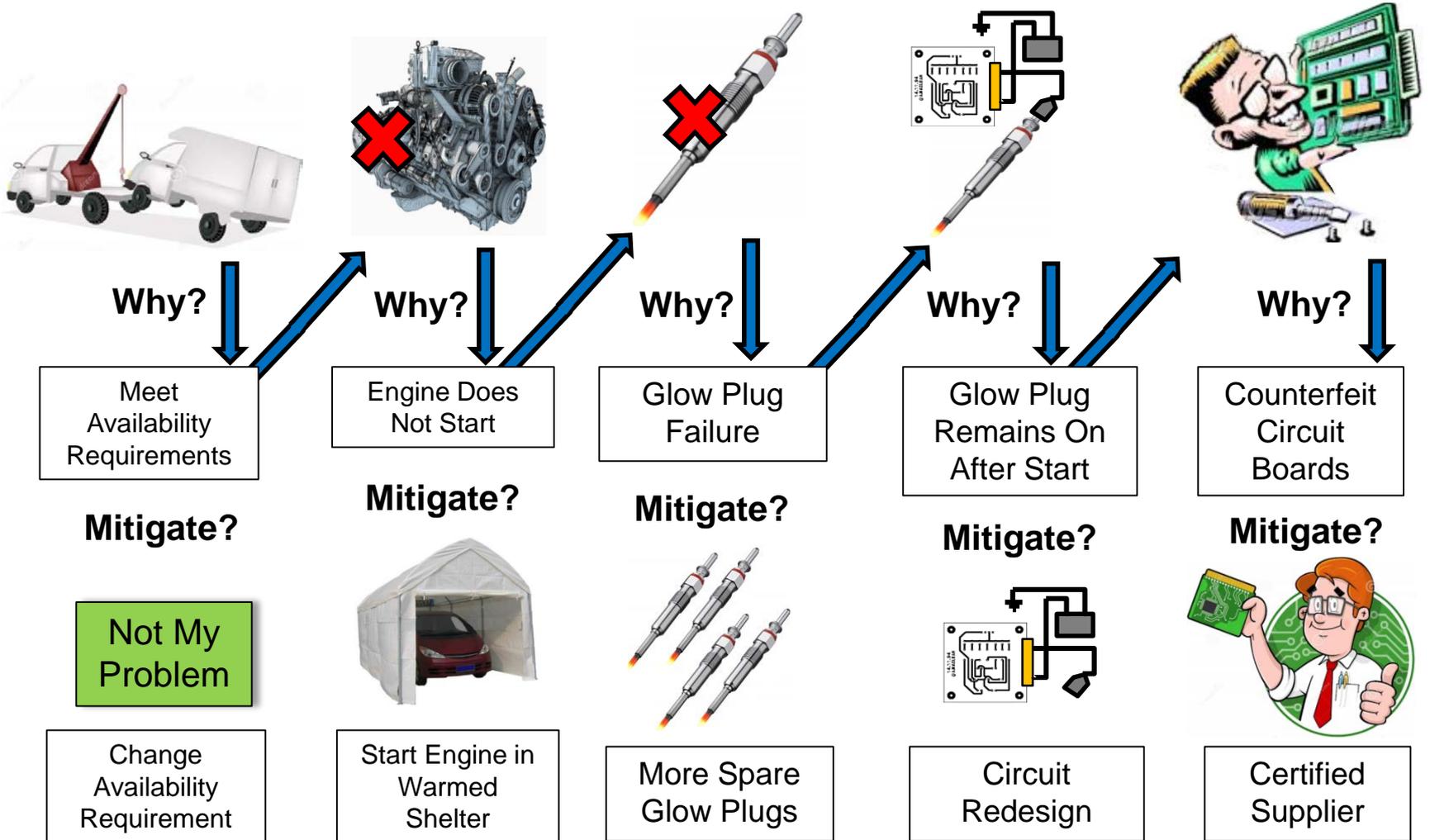
	<u>When?</u>	<u>Who?</u>	<u>Funding?</u>
1. Get new/detailed Program A and SW schedules	Jan 12	CC	Yes
2. Identify insertion points for SW updates	May 12	Tech Dir	Yes
3. Work with SW contractor to improve schedule	July 12	You?	No
4. Incentivize SW lab construction for schedule	Oct 12	x	No
5. Identify root cause of SW technical issues	x	x	x
6. Correct SW technical issues	x	x	x
7. Improve SW schedule by 2 months	x	x	x
8. Improve SW lab construction by 1 month	x	x	x
9. New SW dates coordinated with Program A leadership	x	x	x



MITIGATION TRACKING TOOL BURNDOWN or WATERFALL



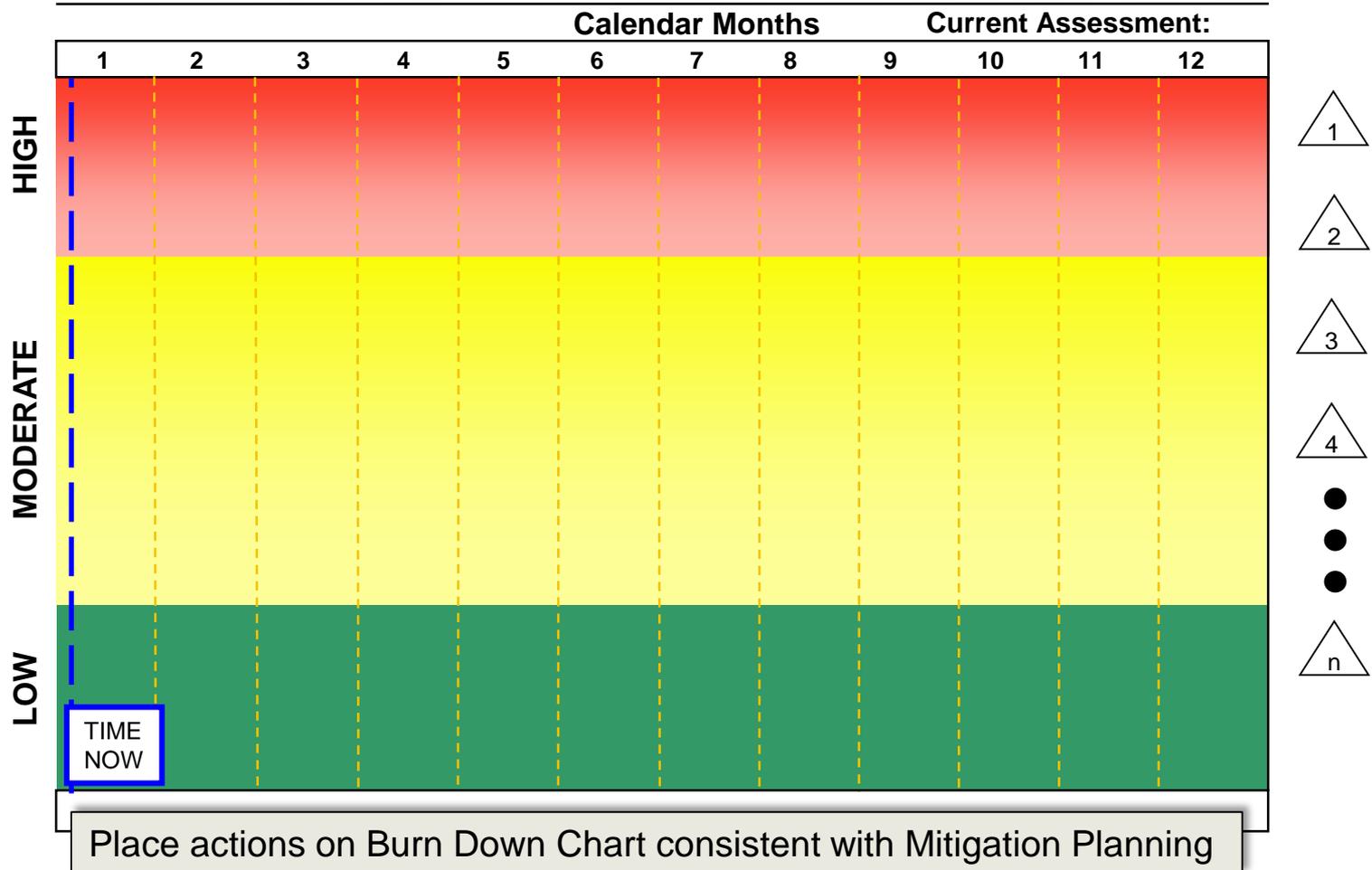
RISK HANDLING?



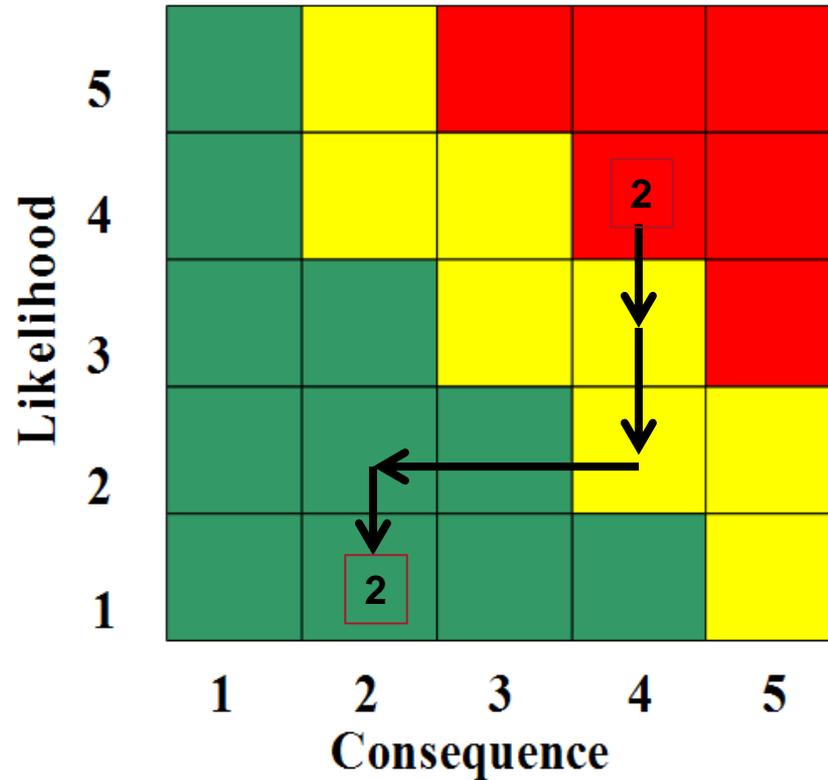
EXERCISE: RISK HANDLING



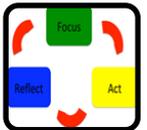
BURN DOWN TEMPLATE



RISK MATRIX TEMPLATE

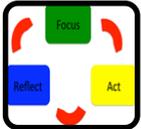


Adjust Risk Matrix Expectation consistent with Mitigation Planning



BURN DOWN ACTIONS TEMPLATE

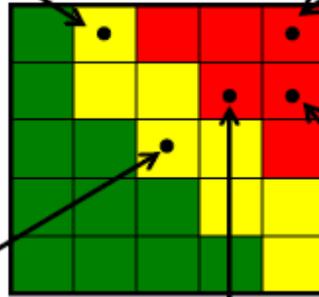
Action	When?	Who?	Funding?
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			



RISK REPORTING MATRIX

- Risk ID Number: 31
- Risk Driver:
- Risk Mitigation Action:
 - Cost: \$
- Closure Date:
- Cost Impacts:
 - RDT&E: \$ or %
 - Production: \$ or %
- Schedule Impacts:
 - Months:
- Performance Impacts:
 - Only achieves XX% of aaa KPP performance

- Risk ID Number: 99
- Risk Driver:
- Risk Mitigation Action:
 - Cost: \$
- Closure Date:
- Cost Impacts:
 - RDT&E: \$ or %
 - Production: \$ or %
 - O&M: \$ or %
- Schedule Impacts:
 - Months:
- Performance Impacts:
 - Only YY% of abc KSA performance

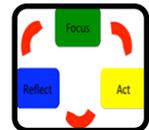


- Risk ID Number: 22
- Risk Driver:
- Risk Mitigation Action:
 - Cost: \$
- Closure Date:
- Cost Impacts:
 - Production: \$ or %
 - O&M: \$ or %
- Schedule Impacts:
 - Months:

- Risk ID Number: 4
- Risk Driver:
- Risk Mitigation Action:
 - Cost: \$
- Closure Date:
- Cost Impacts:
 - Production: \$ or %
- Schedule Impacts:
 - Months:
- Performance Impacts:
 - May trade xyz performance

- Risk ID Number: 18
- Risk Driver:
- Risk Mitigation Action:
 - Cost: \$
- Closure Date:
- Cost Impacts:
 - RDT&E: \$ or %
 - Production: \$ or %
- Schedule Impacts:
 - Months:

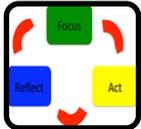
Adjust Risk Reporting Matrix Expectations consistent with Mitigation Planning



RISK REGISTER

Risk Number	Linked WBS/TMS ID#	Owner	Type of Risk	Status	Tier	Risk Event	Likelihood, Consequence Rating	Risk Handling Strategy	Risk Identified Date	Risk Approval Date	Planned Closure Date	Target Risk Rating	Plan Status

Populate Risk Register to reflect Risk Event and Risk Handling

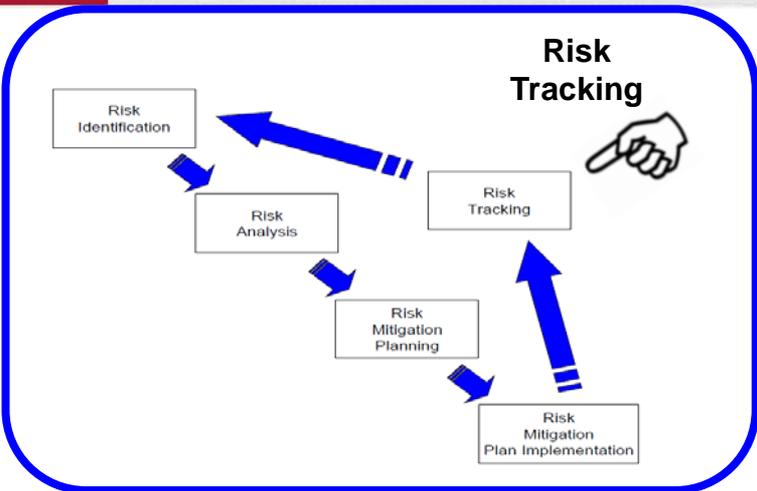


Risk Monitoring

formerly
(Tracking)



RISK MONITORING (TRACKING)



DoD RMG v6.0 2005



RISK MONITORING (TRACKING)

Answers the question: *“How have the risks changed?”*

A means to systematically **track** and **evaluate** risk handling plans against established metrics throughout the acquisition process

Iterative and **recursive** - feeds info back thru risk handling, risk analysis, risk identification, and risk mgt planning steps as warranted



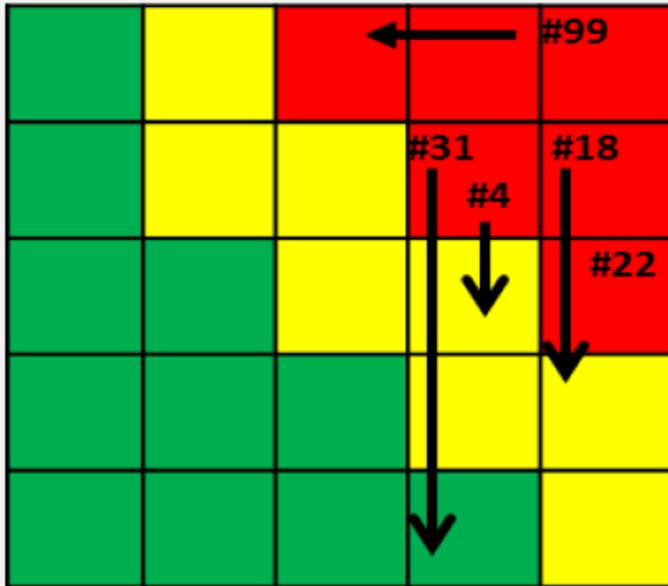
RISK MONITORING

When Monitoring Risks:

- Track the implementation and progress of the risk handling
- TPMs are an integral risk monitoring activity
- Conduct regular status updates to monitor risks for changes to likelihood and/or consequences
- Document active risks as well as those that can be retired - prevent unnoticed relapse of retired risks
- Keep lines of communication open to notify management when ability to handle the risk is ineffective



EXAMPLE RISK MONITORING AND TREND MATRIX



<u>Risk No</u>	<u>Risk Item Description</u>	<u>Risk Trend</u>
31	Risk Title	↓
4	Risk Title	↓
18	Risk Title	↓
99	Risk Title	←
22	Risk Title	Retired

- ↓ = Likelihood decreasing
- ↑ = Likelihood increasing
- ← = Consequence decreasing
- New = New risk added
- Retired = Retired since last report



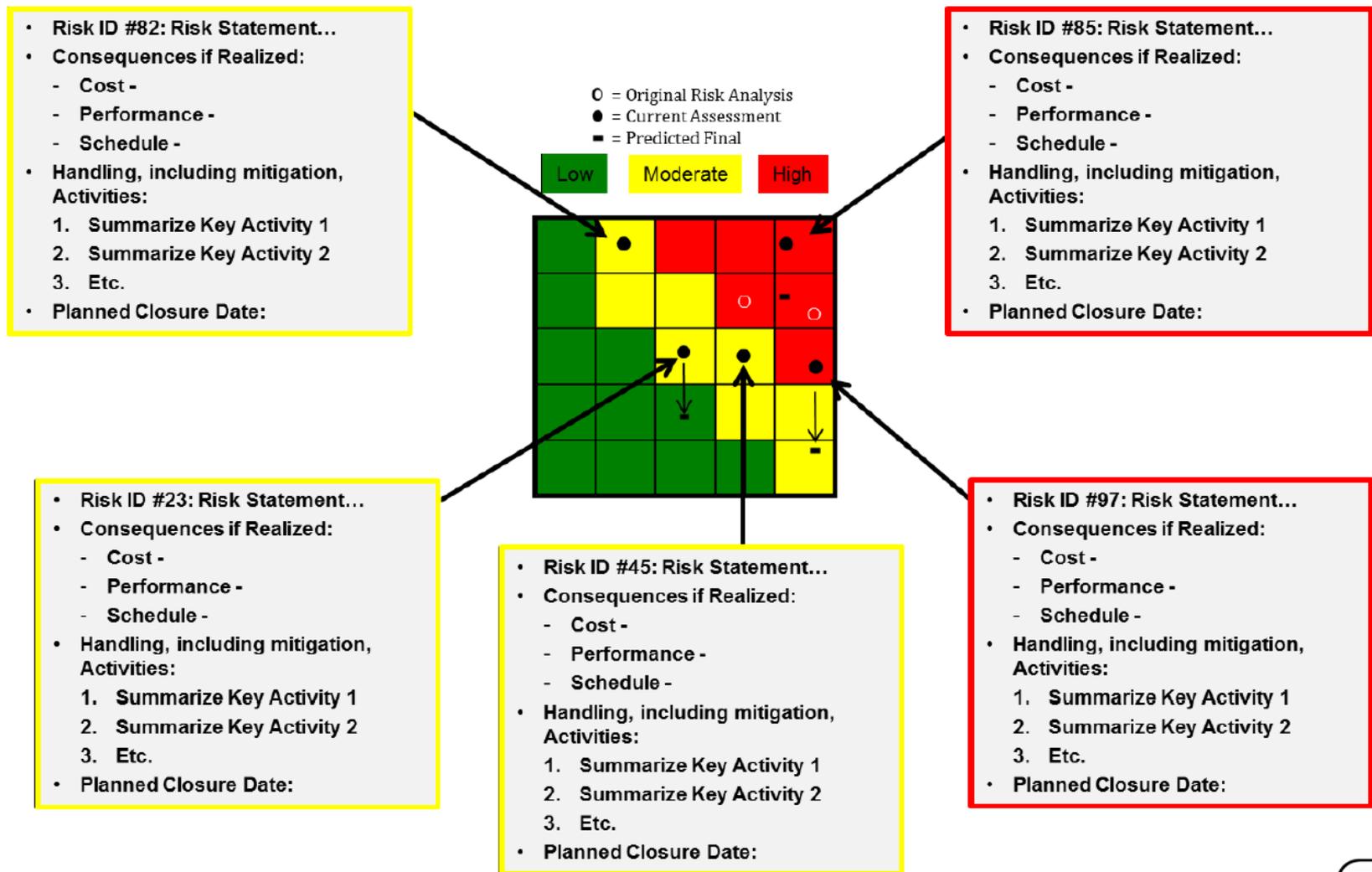


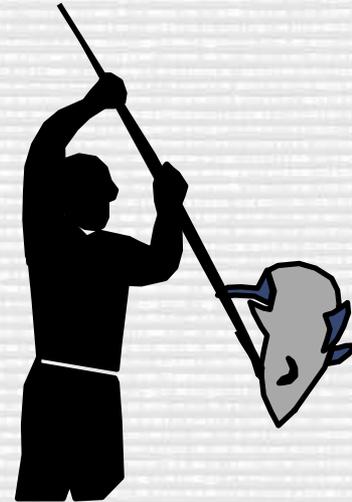
Figure 3-12. Sample Program Tier 1 Risk Reporting Format



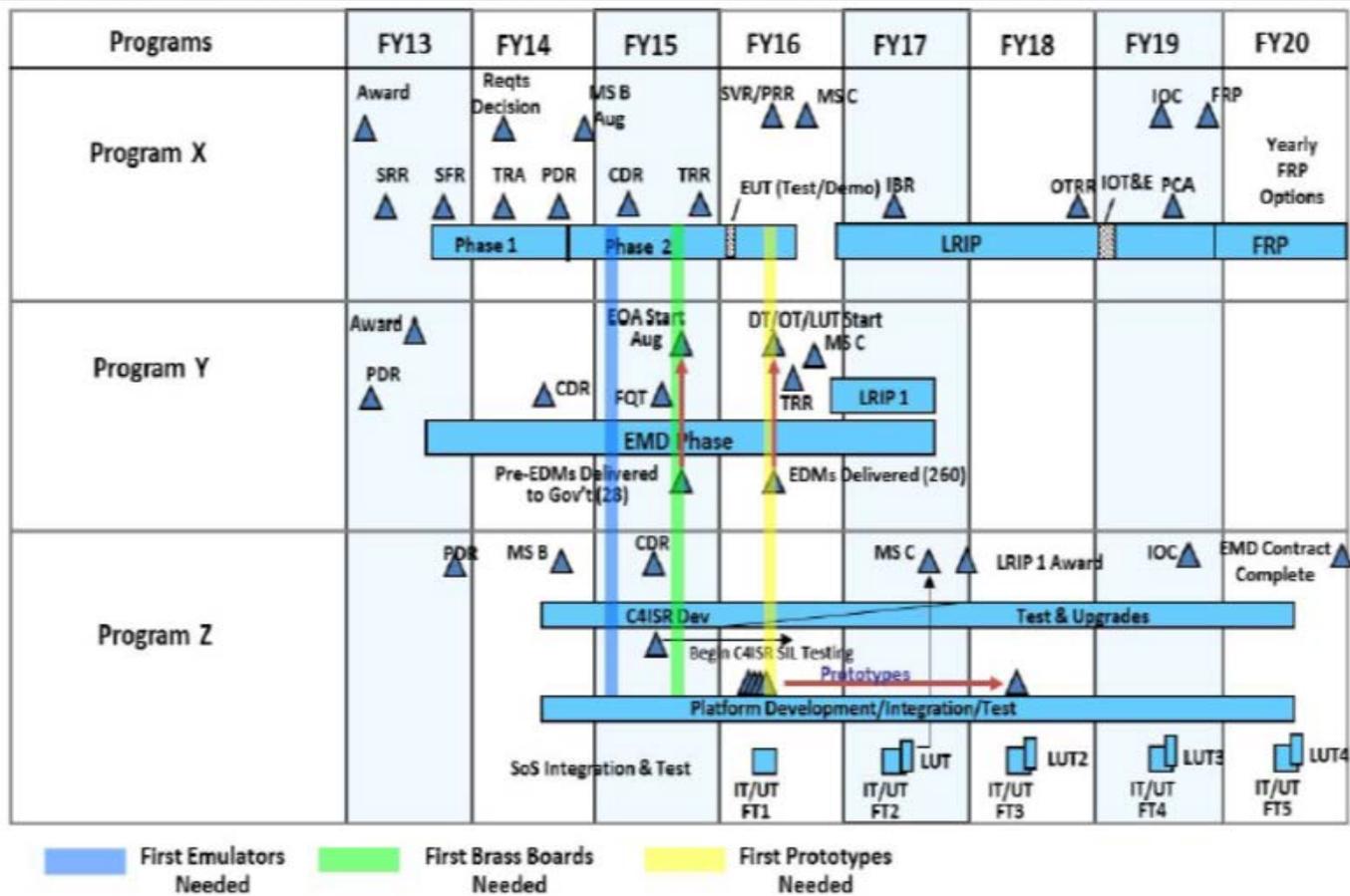
RISK MONITORING EXPECTATIONS

Expectations

- The program team conducts regular status updates to monitor risks for any changes to likelihood or consequence, as well as earned value (cost variance), TPMs, and variation in schedule as a result of program progress.
 - PMOs and contractors establish a regular schedule for reviewing risks.
 - Team alerts management when risk handling plans should be implemented or adjusted.
- Alert the next level of management when ability to handle a risk exceeds the lower level's authority or resources.
- Program team tracks actual versus planned implementation of progress against the risk handling plan.
 - Program establishes a management indicator system over the entire program to monitor risk activity.
 - Program reviews closed risks periodically to ensure their risk level has not changed.



CROSS-PROGRAM RISKS (SCHEDULES)



CROSS-PROGRAM RISKS (MANAGEMENT)

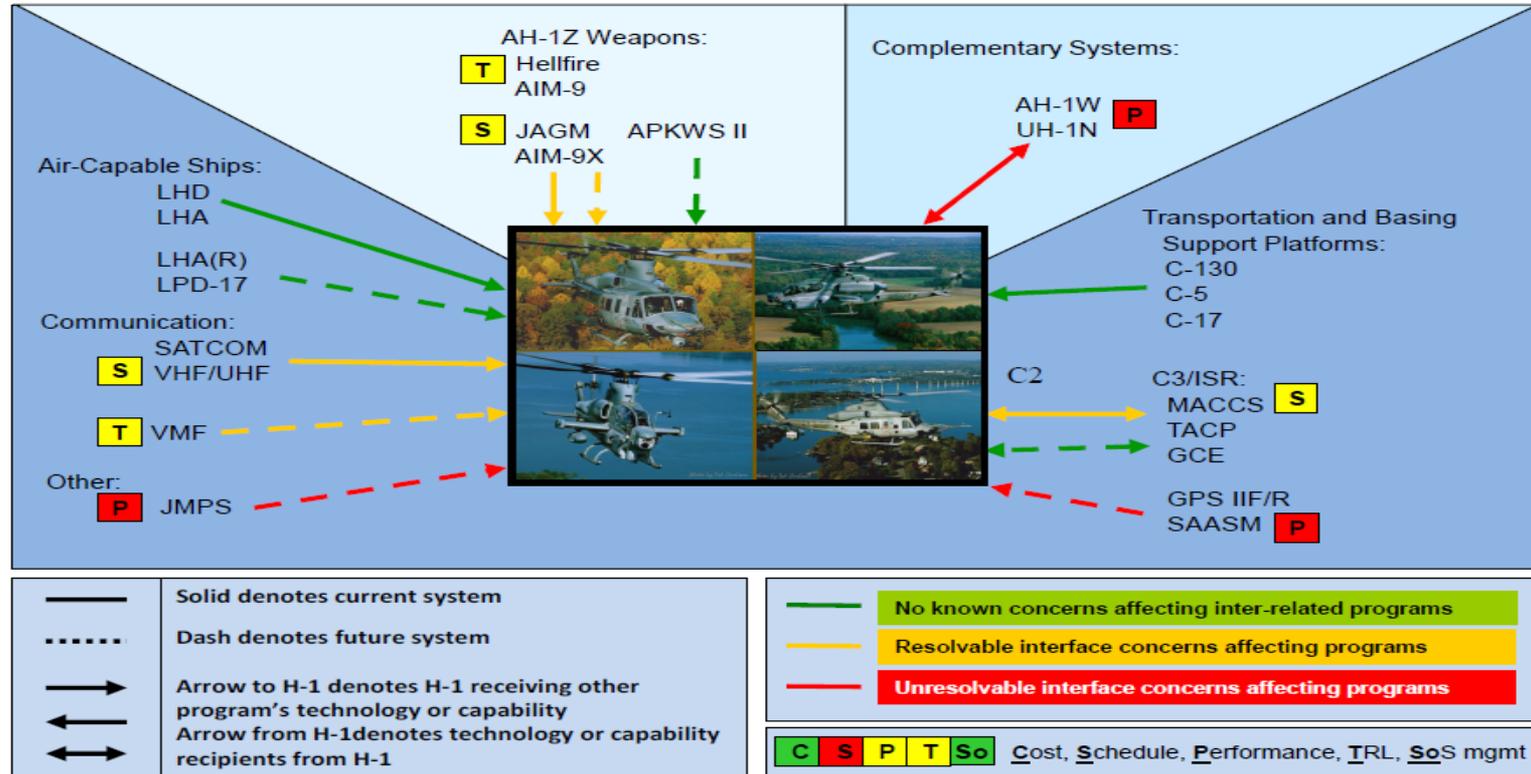


Figure 7-2. Tracking Interdependency Risks



RISK BURN-DOWN

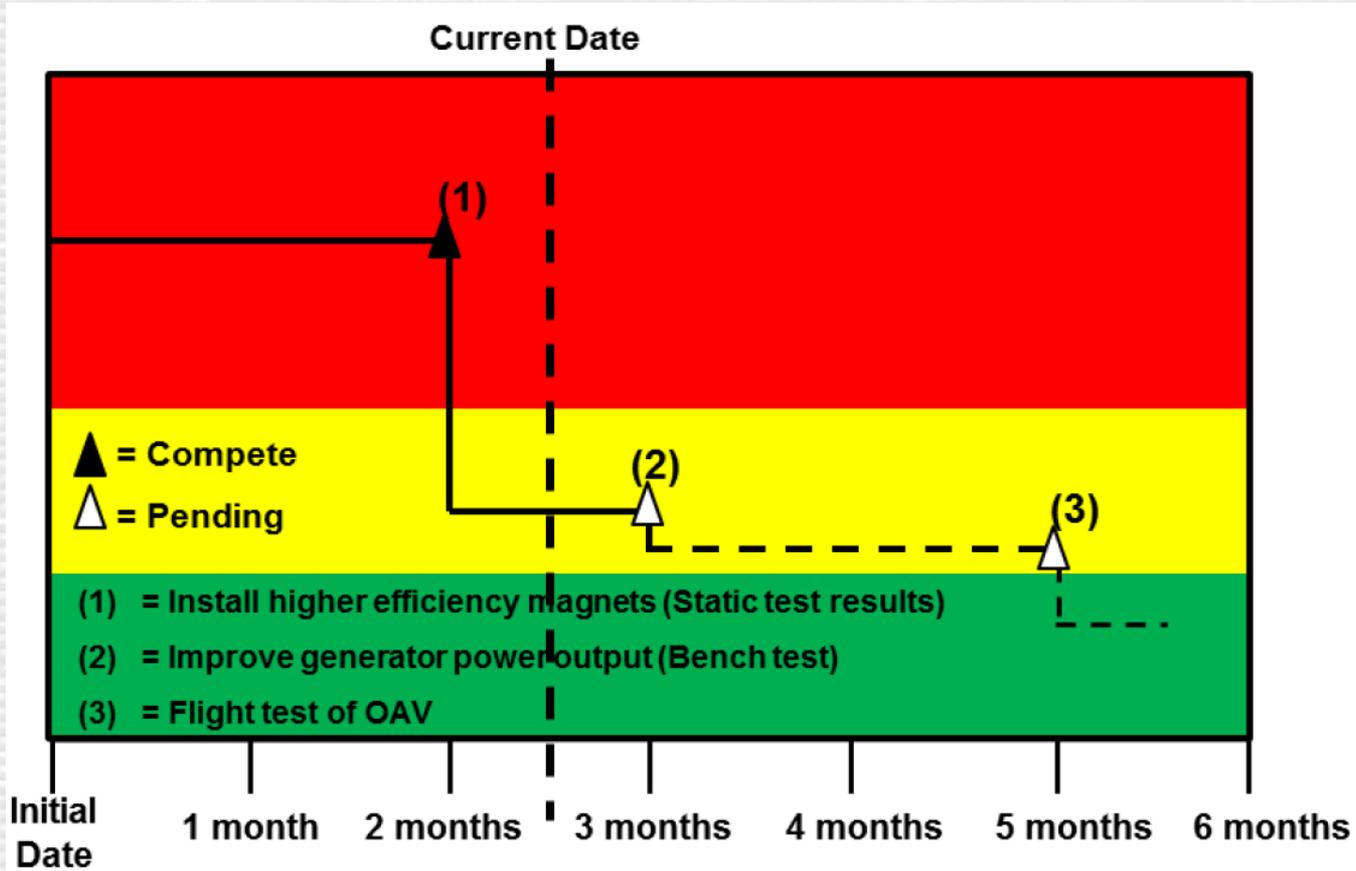


Figure 3-9. Risk Burn-Down



ALTERNATE RISK MATRIX

3. Alternative Risk Reporting Format

Risk	Likelihood (1-5)	Consequences				Performance	Handling Activities	Planned (P) Actual (A)		Closure Date
		Cost			Schedule			Date	Cost	
		RDT&E	Procurement	O&S						
Risk 1 (describe the risk in terms of, "if... (something does or does not occur), then....(negative consequence X and Y will happen)	3	\$450k			4 months	XX performance degraded	1 -Activity XX	(P) 6/16/14 (A)	(P) (A)	(P) 8/12/15
							2 -Activity YYY	(P) 10/12/13 (A) 11/1/13	(P) (A)	(P) (A)
							3 - Activity ZZZ	(P) 8/12/15 (A)	(P) (A)	
Risk 2	4		\$2.2M		8 months		1 -Activity aaa	(P) 7/13/14 (A)	(P) (A)	(P)7/13/14 (A)
							2 -	(P) (A)	(P) (A)	
							3 -	(P) (A)	(P) (A)	
Risk 3	2		\$520K		2 months		1 -	(P) (A)	(P) (A)	(P) (A)
							2 -	(P) (A)	(P) (A)	
							3 -	(P) (A)	(P) (A)	

↑
Insert risk statement in this column

↑
Insert assessed likelihood rating for the risk

↑
Briefly describe the cost, schedule, and performance consequences of the risk

↑
Summarize the key handling activities

↑
Show the planned and actual completion dates and cost for each activity

↑
List the planned and actual risk closure dates



RISK MANAGEMENT TOOLS



**RIGHT TOOLS
RIGHT NOW.**



USAF: AFPAM 63-128

The AF Enterprise-wide Risk Management System (an AF-tailored version of the COTS software “Active Risk Manager (ARM)”) is the current standard AF tool to manage and track program risks across the life cycle.

US Air Force Policy Memorandum



Active Risk Manager is the preferred Risk Management tool all Air Force Acquisition Programs are expected to migrate to.

[US Air Force Policy Memorandum ▶](#)

ARM PMO



Free ARM Licenses Available for all Air Force Acquisition Programs.

[ARM PMO ▶](#)

What is Active Risk Manager (ARM)?



ARM uniquely delivers an integrated approach to identifying, documenting, mitigating, monitoring and analyzing risks and opportunities.

[Active Risk Manager \(ARM\) ▶](#)



<http://www.activerisk.com/usaf/>



PMT 257_DAY 4_RISK MANAGEMENT TOOLS ACTIVE RISK MANAGER

Description

Active Risk Manager (ARM) is a comprehensive enterprise risk management (ERM) software package, in use in over 170 of the globe's most respected and demanding organizations, projects and supply chains.



Features

- Extensive range of ERM capabilities
- Management of project and program risk
- Strategic enterprise oversight
- Delivers an integrated approach to identifying, documenting, mitigating, monitoring and analyzing risks and opportunities in all business functions
- Easily configured to support a range of business domains and processes
- A single web-based system for managing risks and opportunities can be used
- Integration of risk management across operations and projects
- Replaces silo-based, spreadsheet approach to risk management with a single integrated ERM system
- Provides top-down, bottom-up and cross organizational views of risks and opportunities

Active Risk

<http://www.activerisk.com/solutions/active-risk-manager-arm/>



Description

Oracle Crystal Ball is a spreadsheet-based application suite for predictive modeling, forecasting, simulation, and optimization. It gives insight into the critical factors affecting risk.

The screenshot shows a spreadsheet window titled 'ClearView Project' with the following data:

Costs (in millions):	
Development Cost of ClearView to Date	\$10.0
Testing Costs	\$3.9
Marketing Costs	\$16.5
Total Costs	\$30.4
Market Study (in millions):	
Persons in U.S. with Nearsightedness Today	40.0
Growth Rate of Nearsightedness	2.00%
Persons with Nearsightedness After One Year	40.8
Gross Profit on Dosages Sold:	
Market Penetration	7.28%
Profit Per Customer in Dollars	\$12.00
Gross Profit if Approved (MM)	\$35.7
Net Profit (MM)	\$5.2

Features

- Uses Monte Carlo Simulation
- Identify and mitigate the key inputs that drive risk
- Automatically calculates and records the results of thousands of different "what if" cases
- Analysis presents range of possible outcomes, their probability of occurring, the inputs that most impact your model, and where you should focus your efforts
- Allows you to work as a team, sharing models and data
- Uses spreadsheet technology that you already own
- Allows you to share your findings through graphs, charts, and reports that present and communicate the results of your analyses

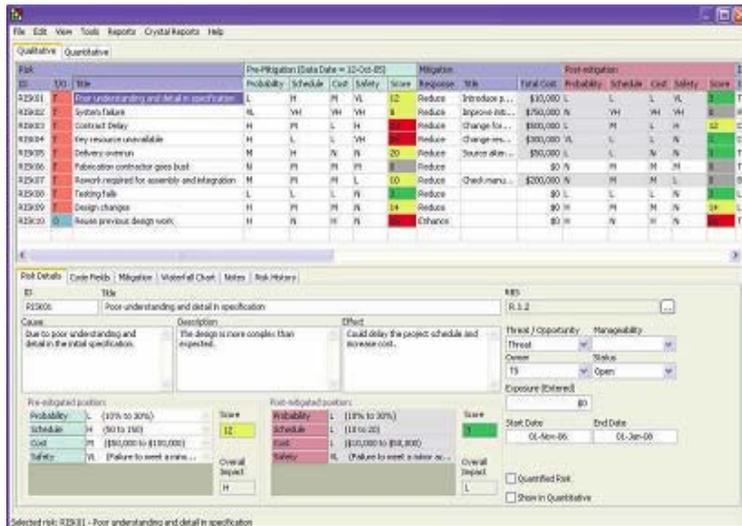
Crystal Ball

<http://www.oracle.com/us/products/middleware/bus-int/crystalball/index-066566.html>



Description

Oracle's Primavera Risk Analysis is a full lifecycle risk analytics solution integrating cost and schedule risk management.



Features

- Helps identify common scheduling pitfalls that may result in misleading schedule or risk analysis results
- Integrates pre-developed risk registers and defines new risk registers
- Addresses full lifecycle risk management through advanced Monte Carlo-based cost and schedule analytics
- Reports confidence levels with regards to finish dates, costs, float, internal rate of return and net present value
- Integrates project schedules and cost estimates to model risks and uncertainty
- Determines contingency and risk response plans
- Provides a comprehensive means of reporting project confidence levels
- Risk-loads projects through risk registers and risk templates before using Monte Carlo simulation to analyze them
- Provides variety of reports, including risk histograms, tornados, and scatter plots

Primavera Risk Analysis

<http://www.oracle.com/us/products/applications/042371.htm>



	@Risk	Risk Radar® Enterprise	Active Risk Manager	Crystal Ball	Primavera Risk Analysis
Microsoft Project Integration?	No	No	Yes	Yes	Yes
Microsoft Excel Integration?	Yes	No	Yes	Yes	---
Use of graphs and charts?	Yes	Yes	Yes	Yes	Yes
Monte Carlo Simulation?	Yes	No	---	Yes	Yes
Customizable Features?	Yes	Yes	Yes	Yes	---
Web-based?	No	Yes	Yes	Yes	Yes
What stands out?	<ul style="list-style-type: none"> • Simulations are calculated 100% within Excel. •Compatibility: Compatible with PC Excel 2000 and higher and PC Windows 2000 and higher. 	<ul style="list-style-type: none"> • Supports guidance from the PMI PMBOK®, IEEE, SEI CMMI and DoD Risk Management Guide for DoD Acquisition •NMCI Certified; ATO Army EIS network •Compatible with MySQL 5 or newer, Oracle 8ior newer , SQL Server 2000 or newer. Used by Govt contractors and Govt agencies. 	<ul style="list-style-type: none"> • Compatible with Microsoft SQL Server and Oracle databases, Microsoft Reporting Services and SharePoint. •Interfaces with Microsoft Excel, Microsoft Project, Primavera, Telelogic DOORS and Cradle. 	<ul style="list-style-type: none"> • Compatible with Microsoft Excel 2002 (XP), 2003 with Service Pack 3, or Microsoft Excel 2007 with Service Pack 2, Microsoft Internet Explorer 7.0 and 8.0. 	---
Possible shortcomings	---	<ul style="list-style-type: none"> • Oracle database requires a separate 3rd party driver. 	---	---	---

--- indicates no data found



DAU RM WORKSHOP OVERVIEW

Risk Management Overview

Risk Management Process

- Planning
- Identification
- Analysis
- Handling (Mitigation)
- Monitoring (Tracking)
- Tools

Issue Management

Opportunity Management

Next Steps



DAU RISK MANAGEMENT WORKSHOP NOTIONAL AGENDA

One Day Workshop

Intro	Risk Planning	Risk ID	Lunch	Risk Analysis	Risk Handling	Risk Monitoring
-------	---------------	---------	-------	---------------	---------------	-----------------

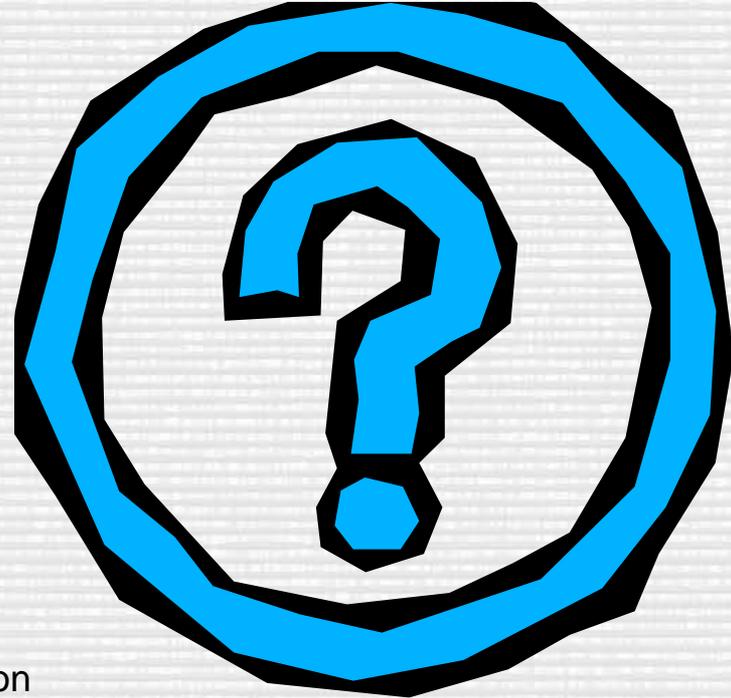
Two Day Workshop

Intro	Risk Cluture	Risk Planning	Lunch	Risk ID Part 1	Risk ID Part 2
Risk Analysis	Risk Handling Part 1	Lunch	Risk Handling Part 2	Risk Monitoring	Risk Tools



Intended to use actual Program Data with Intact Teams to jump-start / invigorate Risk Management activities to enable program success.

QUESTIONS



Professor Seth Shepherd
Systems Engineering/Test Department
Defense Acquisition University (DAU) – South Region
seth.shepherd@dau.mil
256-922-8751