DoD Risk Management Process

DAU Web Event

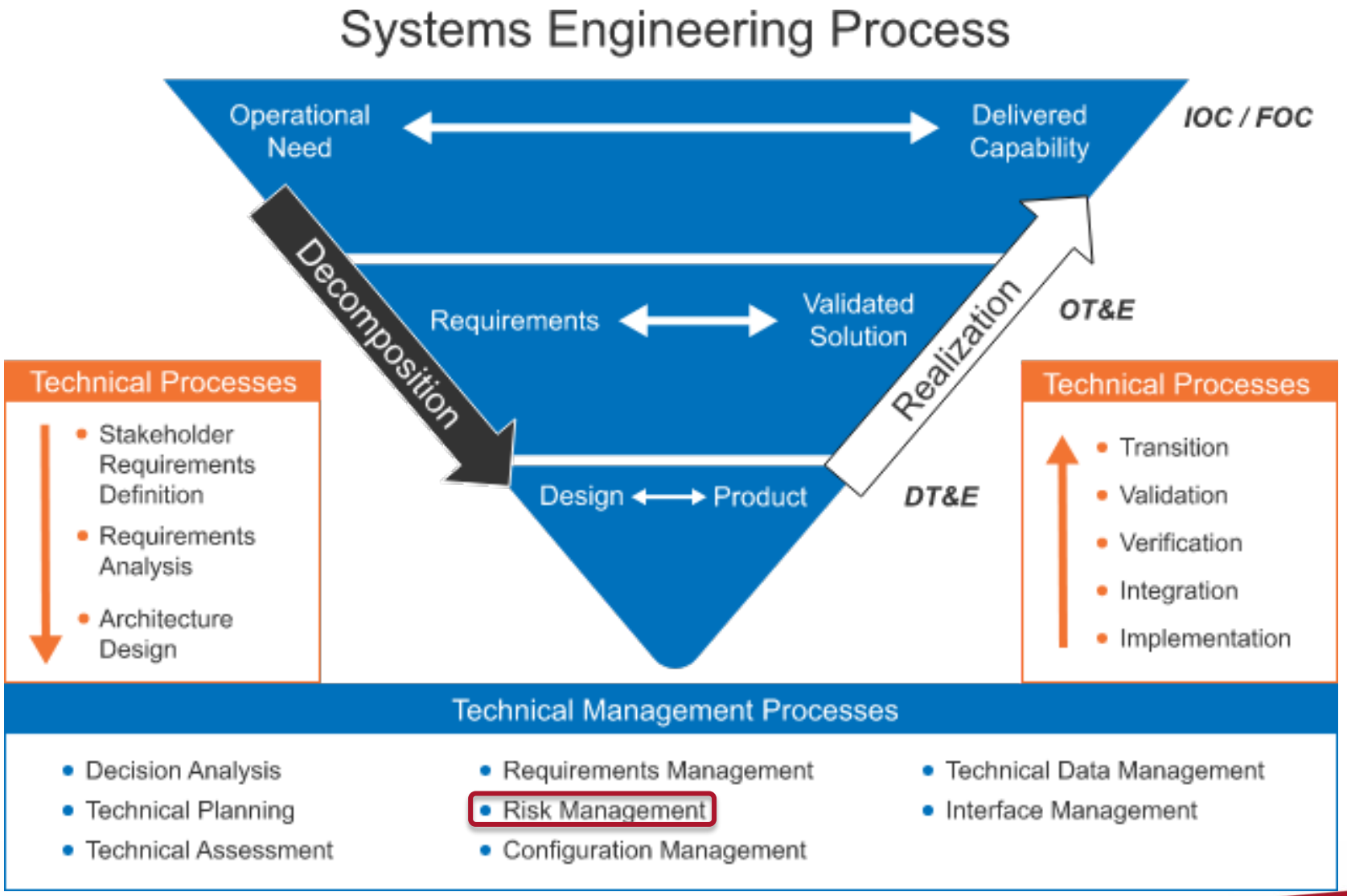
5 April 2023

Mr. Darren Rhyne
Professor of Engineering Management
Capital & Northeast Region
Cell: 571-255-9824
Darren.rhyne@dau.edu

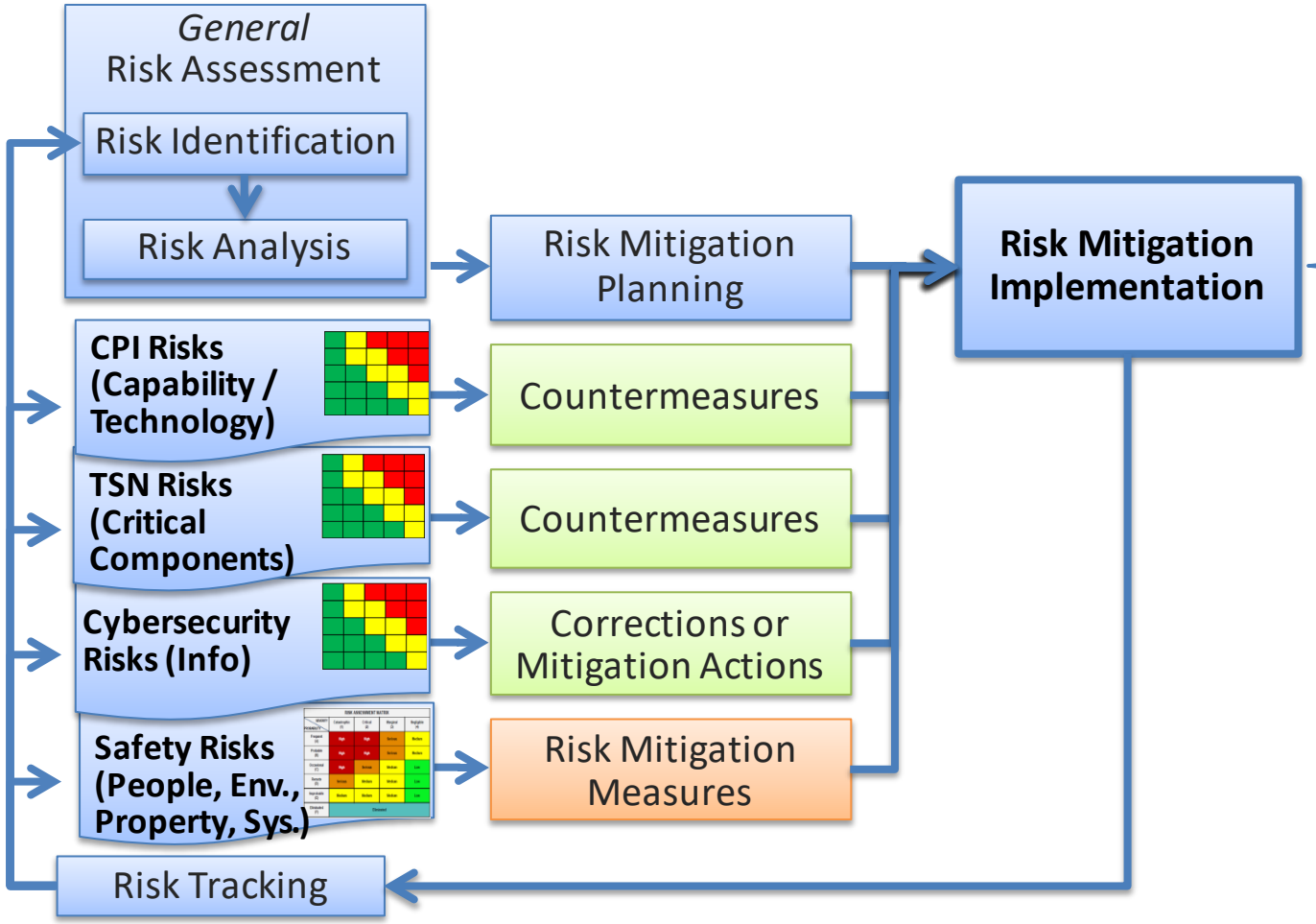
Outline

- Introduction
- DoD Risk Management Process
  - Risk Process Planning
  - Risk Identification
  - Risk Analysis
  - Risk Mitigation (aka Handling)
  - Risk Monitoring
- Risk Management in the DoD Systems Engineering Plan Outline
- Other types of Risk Management/Assessment: ITRA, System Safety, RMF, SCRM/TSN
- Sources for further study

Risk Management – Foundational Technical Management Process



Integrated Program Risk Management



- All mitigations should be incorporated and prioritized.
- Consider trade-offs against the program constraints.

CPI = Critical Program Information
TSN = Trusted Systems and Networks

The consequences of all risks can be categorized in one of the three categories, i.e., performance, schedule, and cost.

Go to **www.menti.com** and use the code **9426 4030**

Multiple Choice

Lost contact with audience
Press [Activate slide] to refresh connection.
Activate slide

DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (aka "RIO Guide")

Department of Defense
Risk, Issue, and Opportunity Management Guide
for Defense Acquisition Programs

January 2017

Under Revision

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Washington, D.C.

Contents

PREFACE 1

1 INTRODUCTION 3
1.1 Purpose 3
1.2 Scope 4
1.3 Risk Management Overview 4

2 MANAGING RISK BY ACQUISITION PHASE 7
2.1 Planning Considerations 7
2.1.1 Strategy Development 7
2.1.2 Framing Assumptions 8
2.1.3 Integration with Contractor's Processes 8
2.2 Pre-Materiel Development Decision Phase 9
2.3 Materiel Solution Analysis Phase 9
2.3.1 Suggested Activities in the MSA Phase to Reduce Risk 11
2.4 Technology Maturation and Risk Reduction Phase 12
2.4.1 Suggested Activities and Practices in the TMRR Phase to Reduce Risk 13
2.5 Engineering and Manufacturing Development Phase 14
2.5.1 Suggested Activities in the EMD Phase to Reduce Risk 15
2.6 Production and Deployment Phase 15
2.6.1 Suggested Activities in the P&D Phase to Reduce Risk 16
2.7 Operations and Support Phase 16

3 RISK AND ISSUE MANAGEMENT 17
3.1 Risk Process Planning 18
3.2 Risk Identification 19
3.2.1 Risk Identification Methodologies 19
3.2.2 Risk Categories 21
3.2.3 Risk Statement 22
3.2.4 Evaluation of Candidate Risks 23
3.3 Risk Analysis 23
3.3.1 Consequence 24
3.3.2 Likelihood 26
3.3.3 Risk Reporting Matrix 27
3.3.4 Risk Register 30
3.4 Risk Mitigation 31
3.4.1 Risk Acceptance (and Monitoring) 33
3.4.2 Risk Avoidance 33
3.4.3 Risk Transfer 33
3.4.4 Risk Control 34
3.4.5 Risk Burn-Down 35
3.5 Risk Monitoring 36
3.6 Issue Management 40

4 OPPORTUNITY MANAGEMENT 43

5 MANAGEMENT OF CROSS-PROGRAM RISKS 49

APPENDIX A. PROGRAM RISK PROCESS AND ROLES 53
A.1 Program Risk Process 53
A.2 Risk Management Board and Risk Working Group 55
A.3 Selecting a Risk Management Tool 56
A.4 Risk Management Roles and Responsibilities 57
A.4.1 Government Responsibilities 58
A.4.2 Typical Contractor Responsibilities 59
A.4.3 Suggested Tiered Roles and Responsibilities 59

APPENDIX B. RISK MANAGEMENT IN RELATION TO OTHER PROGRAM MANAGEMENT AND SYSTEMS ENGINEERING TOOLS 63
B.1 Work Breakdown Structure 63
B.2 Integrated Master Plans and Integrated Master Schedules 64
B.3 Earned Value Management 66
B.4 Technical Performance Measures and Metrics 66
B.5 Schedule Risk Analysis 67
B.6 Cost Risk Analysis 67
B.7 Performance Risk Analysis 68

APPENDIX C. RISK MANAGEMENT PROCESS VIGNETTE 69

GLOSSARY 75

ACRONYMS 81

REFERENCES 83

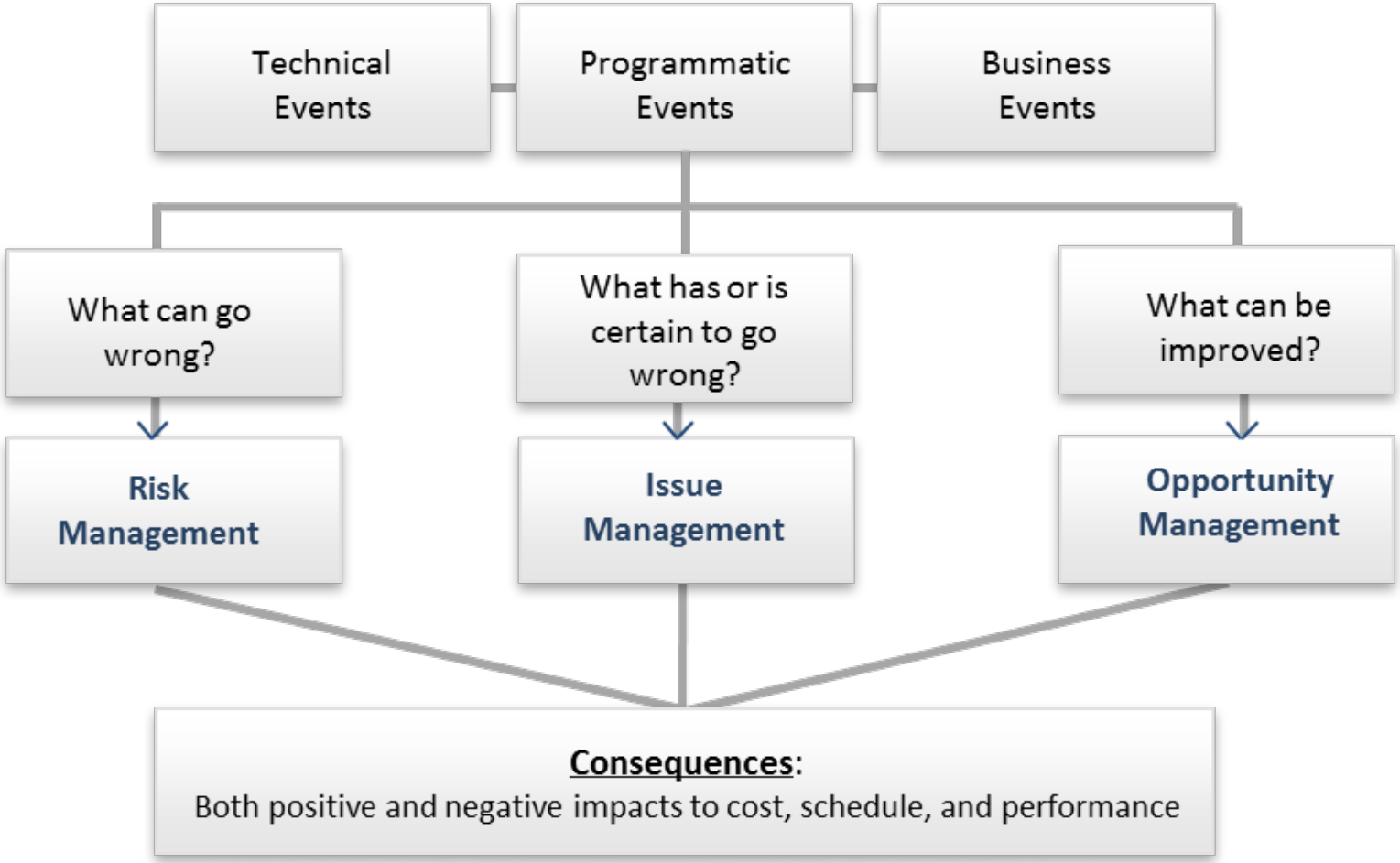
Available on-line through the Systems Engineering & Architecture Website
https://ac.cto.mil/wp-content/uploads/2019/06/2017-RIO.pdf

Risk, Issue, and Opportunity Definitions

- **Risks** are future events or conditions that may have a negative effect on achieving program objectives for cost, schedule, and performance. Risks are defined by (1) the probability (greater than 0, less than 1) of an undesired event or condition and (2) the consequences, impact, or severity of the undesired event, were it to occur.
- **Issues** are events or conditions with negative effect that have occurred (such as realized risks) or are certain to occur (probability of 1) in the future that should be addressed.
- **Opportunities** are potential future benefits to the program's cost, schedule, and/or performance baseline, usually achieved through reallocation of resources.

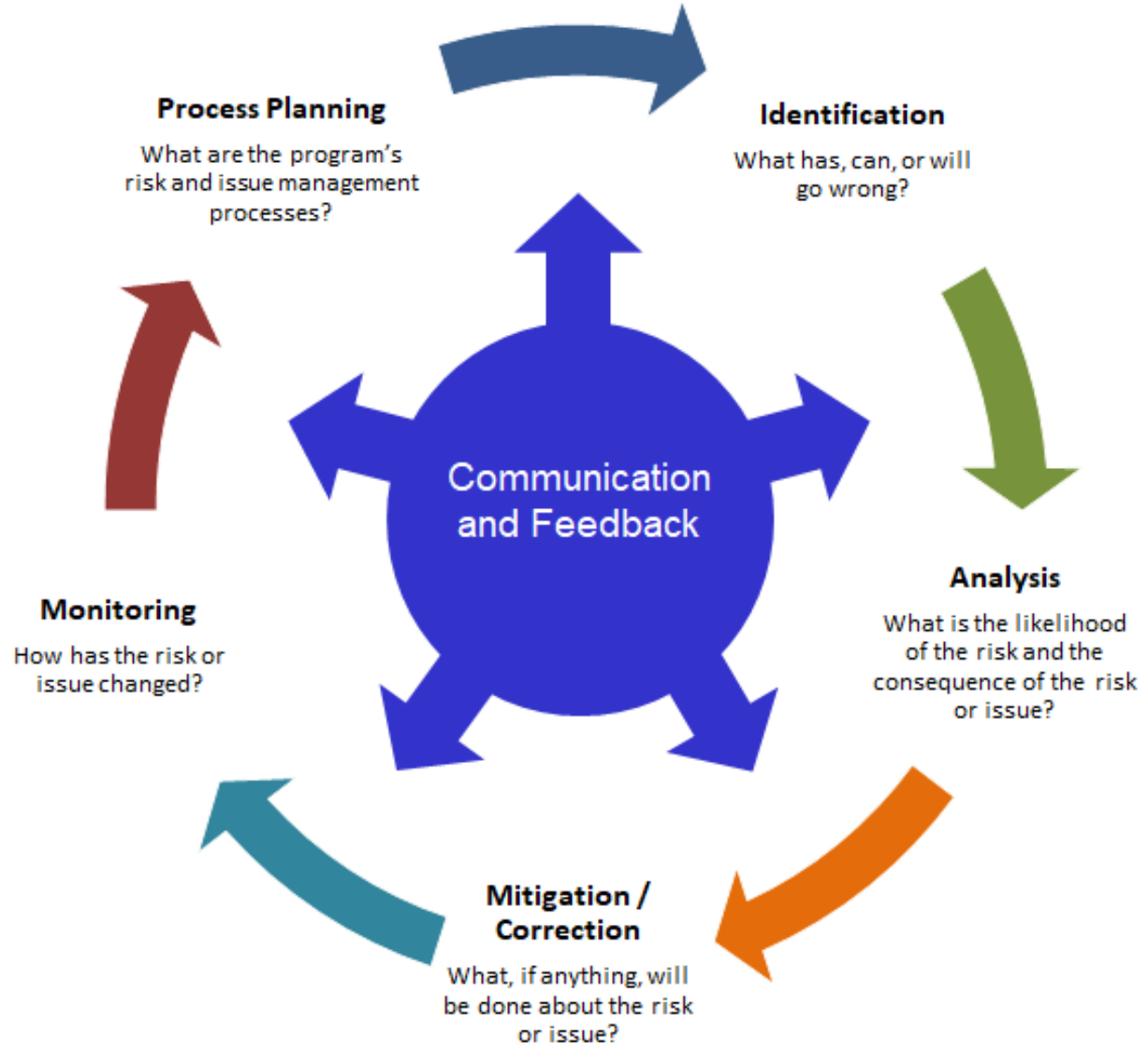
Source: Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, Jan 2017

Risk, Issue, & Opportunity (RIO) Sources



Source: 2017 DoD RIO Management Guide, Figure 1-1, p. 3

DoD Risk (and Issue) Management Process Steps



Source: 2017 DoD RIO Management Guide, Figure 3-1, p. 17

Risk Process Planning

Establish risk processes and procedures:

- Assign roles, responsibilities, and authorities
- Select and document overall approach:
  - Process and procedures
  - Risk analysis criteria for likelihood and consequences
  - Risk mitigation procedures
  - Document in your Program Risk Process, aka Risk Management Plan (ref. App. A.1, RIO Guide)
- Establish traceability of risk to technical requirements and overall program objectives
- Align government and contractor roles, responsibilities, **tools**, and information exchange
- Determine risk management resources, to include budget, facilities, personnel, schedule
- Determine risk management battle rhythm

Source: Adapted from 2017 DoD RIO Management Guide, Figure 3-2, p. 18

Go to **www.menti.com** and use the code **9426 4030**

Which Risk Management tool(s) have y

Lost contact with audience
Press [Activate slide] to refresh connection.
Activate slide

Type in up to three responses.

See [DAU Risk Management CoP Tools tab] for a short summary of various tools.

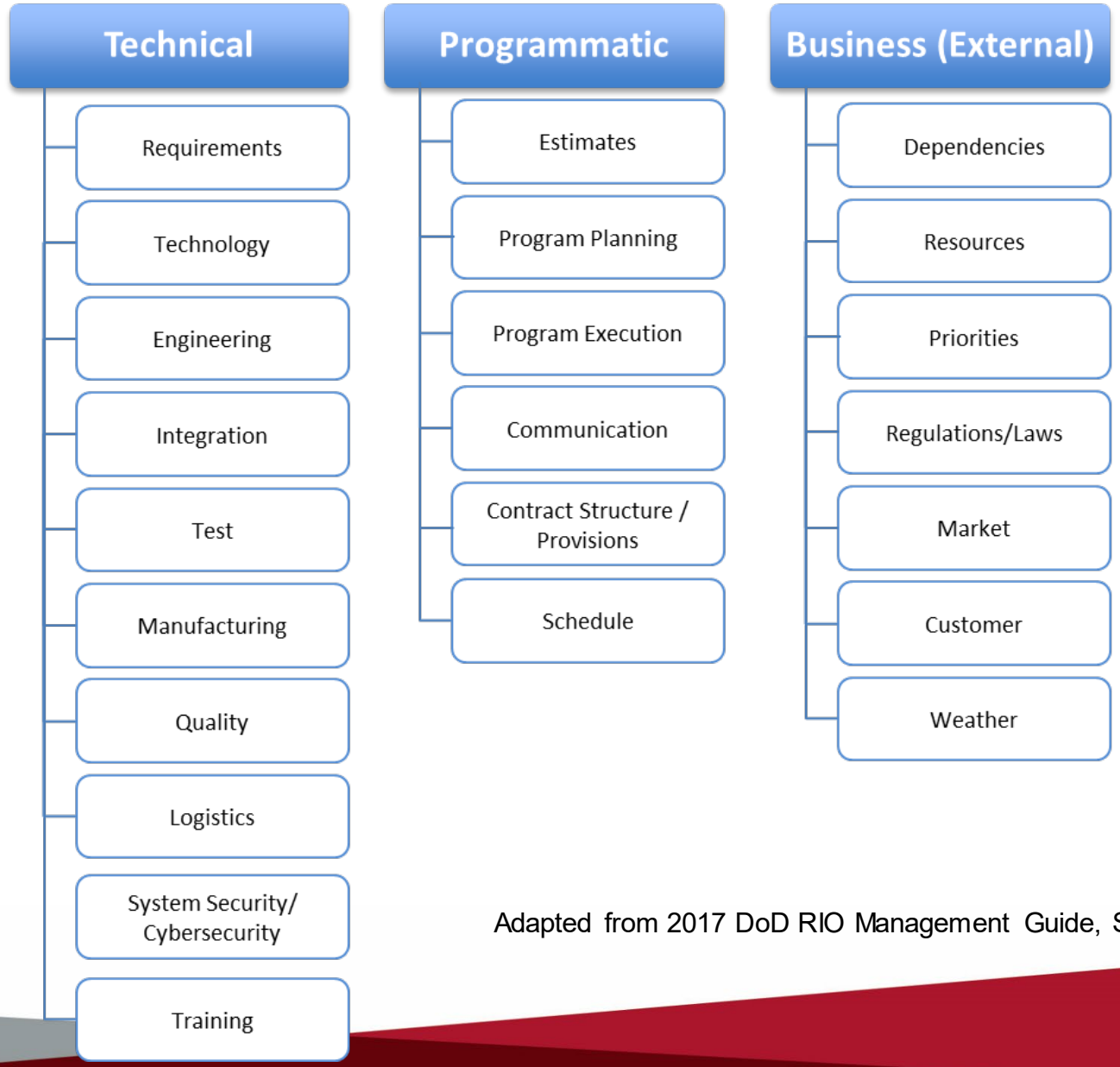
Risk Identification
- What can go wrong?

When identifying risks:

- Understand the nature of the product and the requirements that shape the product
- Use various risk ID methodologies:
  - Independent assessments
  - Brainstorming sessions with SMEs
  - Interviews with IPT leads
  - Review of similar/historical programs
  - Trade studies
- Review analysis of Technical Data, and progress against critical path
- Assess technical performance at all levels: How big a gap? How challenging to cross it?
- What is the root cause of the risk?

Source: Adapted from 2017 DoD RIO Management Guide, Figure 3-3, p. 21

Risk Identification Taxonomy



Adapted from 2017 DoD RIO Management Guide, Sec. 3.2.2, pp. 21-22

Risk Statements

- A good risk statement contains the following elements: (1) the potential event; (2) the associated consequence(s) and the impact(s) to cost (c), schedule (s) and/or performance (p).
  - If known, the risk statement should include an additional element: (3) an existing contributing circumstance (root cause) of the risk.

- As an example, an "if–then" format characterizes the possible risk event or condition and the circumstance/cause (if known) of that risk happening ("if") and the potential consequence(s) and their impact(s) to cost (c), schedule (s) and/or performance (p) ("then").

  - IF some event or condition occurs caused by some circumstance, THEN a specific negative consequence to the program is realized that will result in one or more negative impacts to cost (c), schedule (s), and/or performance (p).

Risk Statements (cont.)

- Example statement using the "if–then" format **without** known cause:
  - IF the engine performance is less than required (risk), THEN engine redesign will have to occur (consequence), causing a X schedule slippage and $Y budget overrun (impacts).

- Example statement using the "if–then" format **with** known cause:
  - IF the engine performance is less than required (risk) due to the requirement to purchase a COTS engine (cause), THEN engine redesign will have to occur (consequence), causing X schedule slippage and $Y budget overrun (impacts).

- When possible, programs should use a single approach to writing risks for consistency and should present each risk in a clear, concise statement.

The risk statement should not include a potential risk mitigation strategy, other solution, or other extraneous information.

More Risk Statement Examples

Here is an example of a type of risk statement you may see or may have seen:

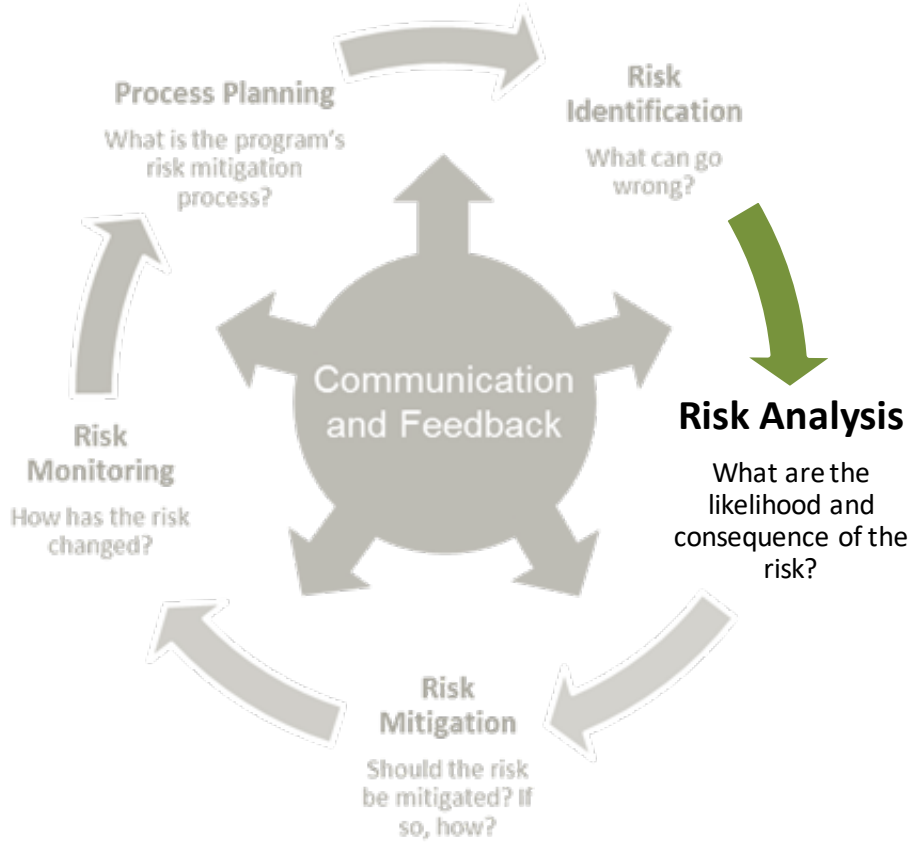
- **If the high vacancy rate in software engineering staff persists, then the program staffing will be inadequate.**
  - This is an overly general statement (with circular logic), could be considered an issue, it provides no impact on program objectives or lends any insight into underlying or existing causal conditions.

The following risk statement is better:

- **If there is a high vacancy rate in software engineering staff due to recruiting by competitors offering higher pay, then the commitment to deliver first software builds will not be met, resulting in "X" months schedule slip.**

Risk Analysis

- How big is the risk?



Source: Adapted from 2017 DoD RIO Management Guide, Figure 3-4, p. 24

When analyzing risks:

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

Typical Likelihood Criteria

The level of likelihood of each root cause is established using specified criteria.

For example, if the root cause has a 50% probability of occurring, the corresponding likelihood is Level 3.

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%

Source: 2017 DoD RIO Management Guide, Table 3-2, p. 26

Sample Consequence Criteria

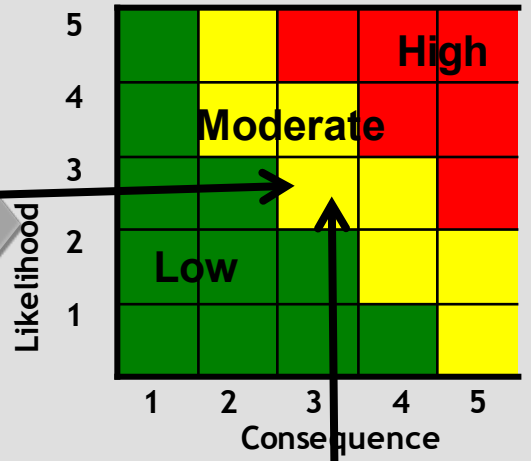
Level	Cost	Schedule	Performance
5 Critical Impact	10% or greater increase over APB objective values for RDT&E, PAUC, or APUC Cost increase causes program to exceed affordability caps	Schedule slip will require a major schedule rebaselining Precludes program from meeting its APB schedule threshold dates	Degradation precludes system from meeting a KPP or key technical/supportability threshold; will jeopardize program success [2] Unable to meet mission objectives (defined in mission threads, ConOps, OMS/MP)
4 Significant Impact	5% - <10% increase over APB objective values for RDT&E, PAUC, or APUC Costs exceed life cycle ownership cost KSA	Schedule deviations will slip program to within 2 months of approved APB threshold schedule date Schedule slip puts funding at risk Fielding of capability to operational units delayed by more than 6 months[1]	Degradation impairs ability to meet a KSA. [2] Technical design or supportability margin exhausted in key areas Significant performance impact affecting System-of System interdependencies. Work-arounds required to meet mission objectives
3 Moderate Impact	1% - <5% increase over APB objective values for RDT&E, PAUC, or APUC Manageable with PEO or Service assistance	Can meet APB objective schedule dates, but other non-APB key events (e.g., SETRs or other Tier 1 Schedule events) may slip Schedule slip impacts synchronization with interdependent programs by greater than 2 months	Unable to meet lower tier attributes, TPMs, or CTPs Design or supportability margins reduced Minor performance impact affecting System-of System interdependencies. Work-arounds required to achieve mission tasks
2 Minor Impact	Costs that drive unit production cost (e.g., APUC) increase of <1% over budget Cost increase, but can be managed internally	Some schedule slip, but can meet APB objective dates and non-APB key event dates	Reduced technical performance or supportability; can be tolerated with little impact on program objectives Design margins reduced, within trade space [2]
1 Minimal Impact	Minimal impact. Costs expected to meet approved funding levels	Minimal schedule impact	Minimal consequences to meeting technical performance or supportability requirements. Design margins will be met; margin to planned tripwires

See acronym definitions in DAU Glossary

Source: 2017 DoD RIO Management Guide, Table 3-1, p. 25

Risk Reporting Matrix & 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%



Level	Cost	Schedule	Performance
5 Critical Impact	10% or greater increase over APB objective values for RDT&E, PAUC, or APUC Cost increase causes program to exceed affordability caps	Schedule slip will require a major schedule rebaselining Precludes program from meeting its APB schedule threshold dates	Degradation precludes system from meeting a KPP or key technical/supportability threshold; will jeopardize program success [2] Unable to meet mission objectives (defined in mission threads, ConOps, OMS/MP)
4 Significant Impact	5% - <10% increase over APB objective values for RDT&E, PAUC, or APUC Costs exceed life cycle ownership cost KSA	Schedule deviations will slip program to within 2 months of approved APB threshold schedule date Schedule slip puts funding at risk Fielding of capability to operational units delayed by more than 6 months [1]	Degradation impairs ability to meet a KSA. [2] Technical design or supportability margin exhausted in key areas Significant performance impact affecting System-of System interdependencies. Work-arounds required to meet mission objectives
3 Moderate Impact	1% - <5% increase over APB objective values for RDT&E, PAUC, or APUC Manageable with PEO or Service assistance	Can meet APB objective schedule dates, but other non-APB key events (e.g., SETRs or other Tier 1 Schedule events) may slip Schedule slip impacts synchronization with interdependent programs by greater than 2 months	Unable to meet lower tier attributes, TPMs, or CTPs Design or supportability margins reduced Minor performance impact affecting System-of System interdependencies. Work-arounds required to achieve mission tasks
2 Minor Impact	Costs that drive unit production cost (e.g., APUC) increase of <1% over budget Cost increase, but can be managed internally	Some schedule slip, but can meet APB objective dates and non-APB key event dates	Reduced technical performance or supportability; can be tolerated with little impact on program objectives Design margins reduced, within trade space [2]
1 Minimal Impact	Minimal impact. Costs expected to meet approved funding levels	Minimal schedule impact	Minimal consequences to meeting technical performance or supportability requirements. Design margins will be met; margin to planned tripwires

Source: 2017 DoD RIO Management Guide, Figure 3-5, p. 28

Documenting Risks in a Risk Register

A risk register is crucial for managing risks. Here is a simple example:

Table 3-4. Risk Register Excerpt

Risk Number	Linked WBS/IMS ID#	Owner	Type of Risk	Status	Risk Event	Likelihood, Consequence Rating	Risk Mitigation Strategy	Risk Identified Date	Risk Approval Date	Planned Closure Date	Target Risk Rating	Plan Status
8231	3.2.2	Name	Technical	Open	Excessive number of priority 1 and 2 software defects may cause a delay to the start of IOT&E	L=3, C=4	Control - Program will apply mitigation reserve to retain adequate software engineers to burn-down SW defects	8/23/2015	1/14/2016	2/12/2016	L=1, C=4	On schedule

Source: 2017 DoD RIO Management Guide, Table 3-4, p. 31

Risk Mitigation (aka Handling)

- What's the plan?

Source: 2017 DoD RIO Management Guide, Figure 3-5, p. 28

When mitigating individual risks consider…

- Is the risk mitigation plan feasible?
- Is the risk mitigation plan affordable in terms of funding and any other needed additional resources?
- Is adequate time available to develop and implement the risk mitigation plan?
- What impact does the risk mitigation plan have on the overall program schedule and on the technical performance of the system?
- Are the expectations realistic given program circumstances, constraints, and objectives?

Consider the Accept, Avoid, and Transfer options, not just the Control option

Risk Mitigation Strategy: Risk Acceptance (and Monitoring)

By accepting the risk, the program acknowledges that the risk event or condition may be realized and the program is prepared to accept the consequences.

What are some conditions in which we would make a conscious decision to accept risk?

- Low likelihood and/or low consequence risk events where DoD is in best position to manage risk.
- Specific response actions are identified if the risk event occurs and resources and schedule are available to implement the plan.
- In constrained environments, programs occasionally must accept risk.
- Sometimes risk is accepted because no feasible mitigation is available.

Accepting a risk does not mean that it should be ignored.

Risk Mitigation Strategy: Risk Avoidance

Through risk avoidance, a program reduces or eliminates the risk event or condition by taking an alternate path. Generally accomplished early in the acquisition process but can occur at any time.

What are some alternate paths to reduce or eliminate risks?

- Replace source of the risk with less risky solution / design / technology
- Change: Allocation of program resources; Requirements; Concept; Specifications; and/or operating Procedures
- Defer a selected capability to a subsequent upgrade or release/increment.

Often involves trade-off decisions during requirements development

Risk Mitigation Strategy: Risk Transfer

Risk transfer includes reassigning or delegating responsibility for tasks to mitigate a risk to another entity. Transfer of risk must also be economically reasonable.

What are some entities we can transfer risk to and how can we transfer risk to them?

- Transfer to another program or government organization
- Through inter-program or organizational agreements
- Transfer across an interface?
- Transfer aspects of risk to a contractor?
- Transfer risk to a third party?

Transference of risk does not eliminate all responsibility and risks must be monitored for potential consequences.

Risk Mitigation Strategy: Risk Control

The risk control option seeks to actively reduce risk on the current path to an acceptable level. Control generally entails taking action to reduce the likelihood and/or the consequence of a risk to as low as practical. Control options:

- Multiple Development Efforts
- Early Prototyping
- Incremental Development
- Reviews, Walk-throughs, and Inspections
- Design of Experiments
- Models and Simulation
- Key Parameter Tracking Systems and Control Boards
- Demonstration Events
- Process Proofing

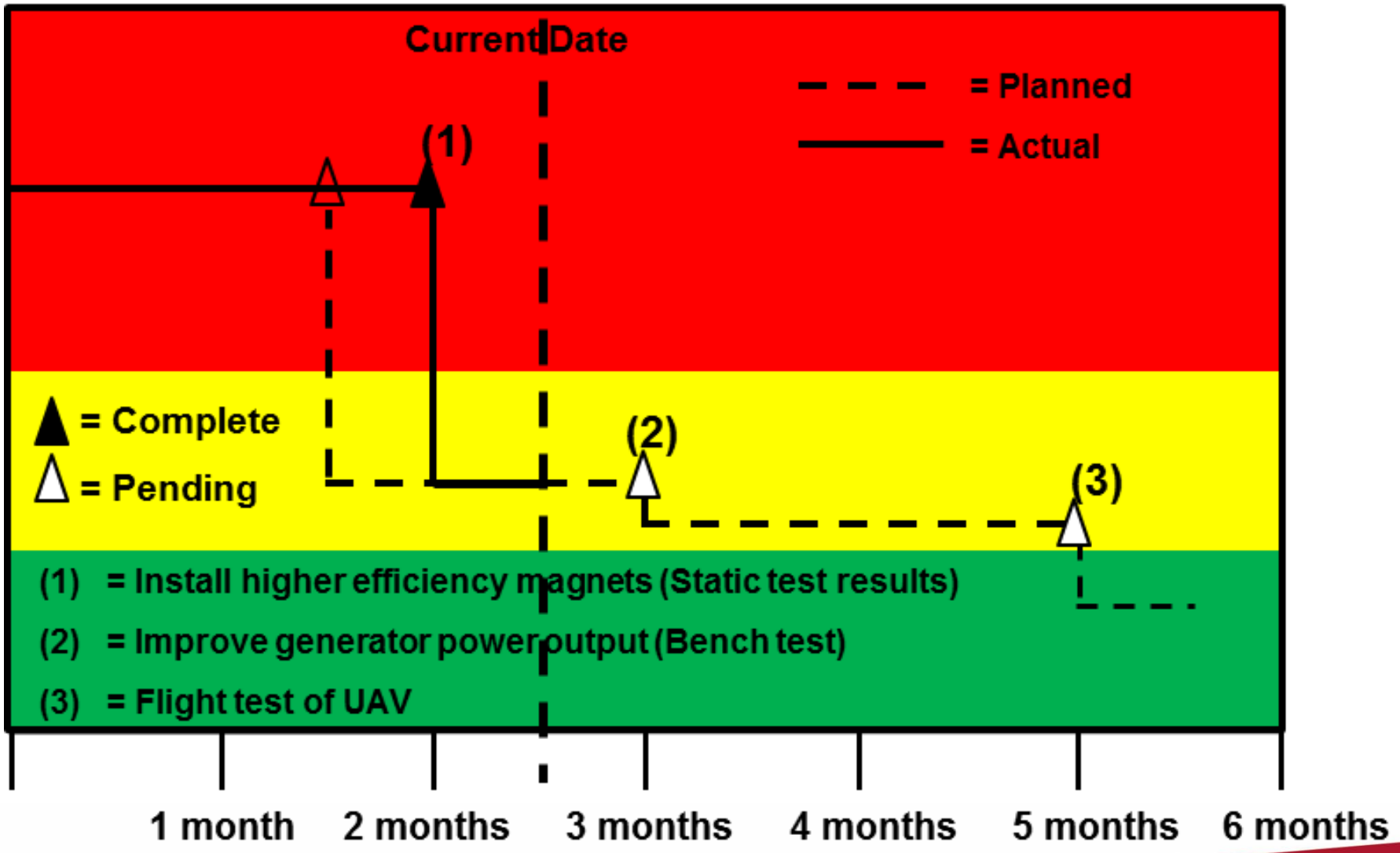
Most common mitigation used in defense programs – reducing risk by trying to manage it with resources. Can be costly and may impact project objectives, such as cost control or schedule performance.

Go to **www.menti.com** and use the code **9426 4030**

Which form of risk mitigation/handling have you used or seen used most often?

Mentimeter

Risk Burn Down



Source: 2017 DoD RIO Management Guide, Figure 3-8, p. 36

Risk Monitoring
- How has the risk changed?

When monitoring risks:

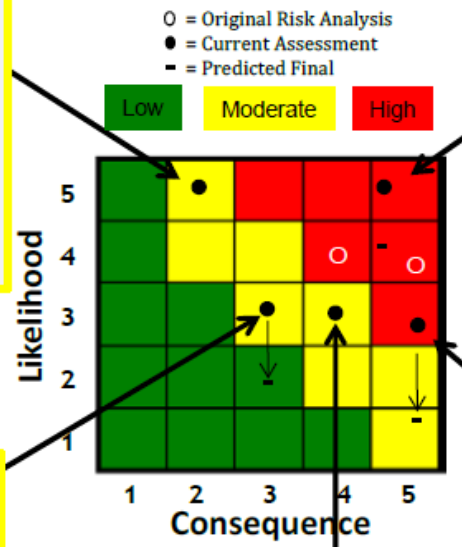
- Track the implementation and progress of the risk mitigation activities
- Include Technical Performance Measures as an integral activity when monitoring risks
- Conduct regular status updates to monitor risks for changes to likelihood and/or consequences
- Document risks that can be retired as well as risks that are still being mitigated to prevent an unnoticed relapse of the retired risk
- Keep lines of communication open to notify management when ability to mitigate the risk is ineffective

Source: Adapted from 2017 DoD RIO Management Guide, Figure 3-9, p. 37

Suggested Risk Reporting Format Over Time

- Risk ID #82: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #85: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:



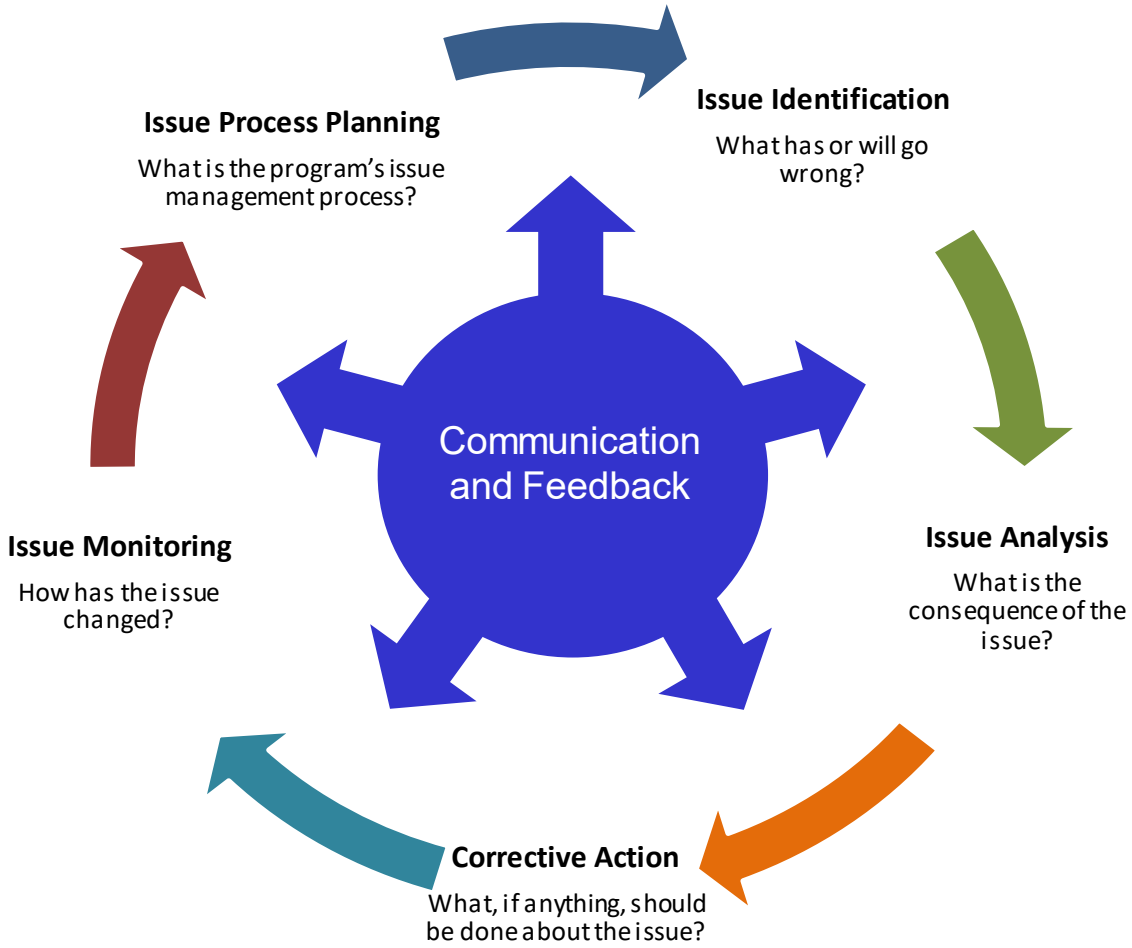
- Risk ID #23: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #45: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #97: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

Source: 2017 DoD RIO Management Guide, Figure 3-11, p. 39

DoD Issue Management Process Steps



Source: 2017 DoD RIO Management Guide, Figure 3-12, p. 40

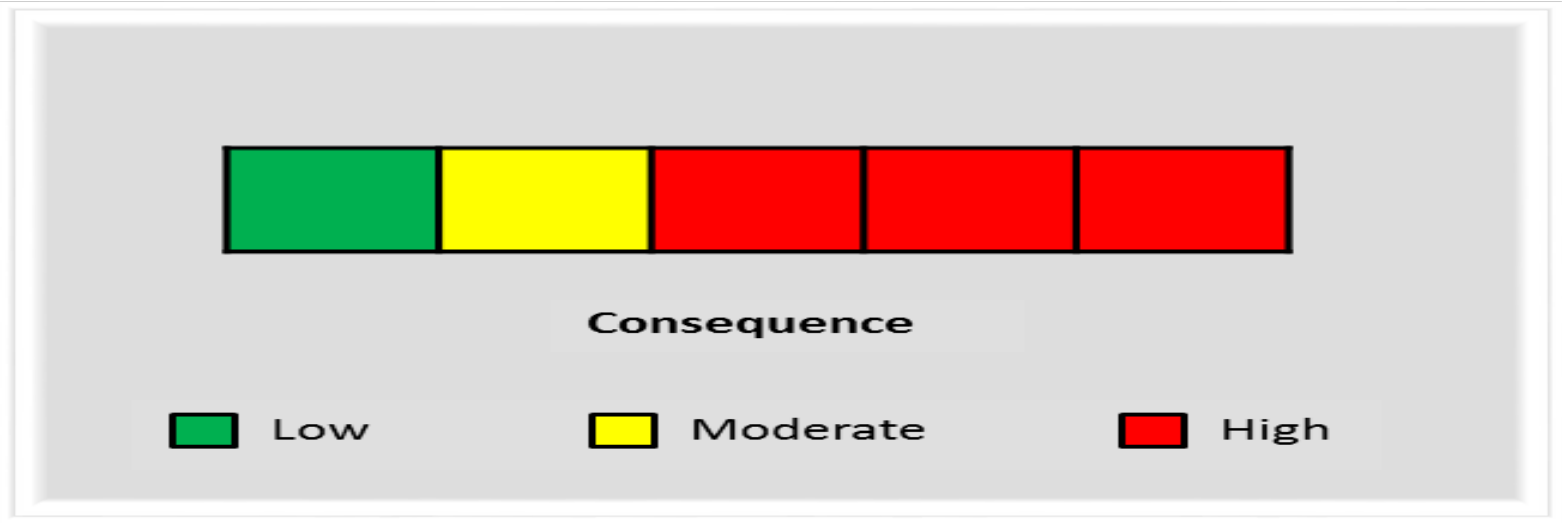
Issues – 100% Occurrence Now or in the Future

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

- Issue management, on the other hand, applies resources to address and resolve a past or occurring event and its related consequences.
  - These events should be cataloged as issues and should be addressed within the program's normal issue management process.
  - In addition, even though an issue may introduce a likely future consequence, this does not make it a risk.
  - To ensure issues and risks are properly identified, programs should have an issue management approach to identify problems and track associated closure plans.
  - Programs should also assess whether issues are spawning prospective risks.

Issue Identification and Consequence Scale

- Issues are best identified before the beginning of a new project or contract and should be updated and reviewed periodically throughout the life cycle of the program.
- Unlike opportunities and risks, there is no assessment of their likelihood because issues have either already occurred or are in the process of occurring (e.g., 100% likelihood).



Source: 2017 DoD RIO Management Guide, Figure 3-13, p. 41

Issues – Corrective Action

- **Ignore:** Accept the consequences without further action based on results of a cost/schedule/performance business case analysis or
- **Control:** Implement a plan to reduce issue consequences and residual risk to as low a level as practical or minimize impact on the program. This option typically applies to high and moderate consequences issues.

Less common options include

- **Avoid:** Eliminate the consequence of the event or condition by taking an alternate path.
  - Examples may involve changing a requirement, specification, design, or operating procedure.
- **Transfer:** Reassign or reallocate the issue responsibility from one program to another, between the government and the prime contractor, within government agencies, or across two sides of an interface managed by the same organization.

DoD Opportunity Management Process Steps

An opportunity is the potential for improving the program in terms of cost, schedule, and performance.

Source: 2017 DoD RIO Management Guide, Figure 4-2, p. 44

Notional Opportunity Register

Opportunity	Likeli-hood	Cost to Implement	Return on Investment					Program Priority	Management Strategy	Owner	Expected Closure
			Monetary			Schedule	Performance				
			RDT&E	Procurement	O&M						
Opportunity 1: Procure Smith rotor blades instead of Jones rotor blades.	Mod	$3.2M			$4M	3 month margin	4% greater lift	#2	Reevaluate - Summarize the mitigation plan	Mr. Bill Smith	March 2017
Opportunity 2: Summarize the opportunity activity.	Mod	$350K	$25K		$375 K			#3	Reject	Ms Dana Jones	May 2017
Opportunity 3: Summarize the opportunity activity.	High	$211K		$0.4M	$3.6 M	4 months less long-lead time needed		#1	Summarize the mitigation plan to realize the opportunity	Ms. Kim Johnson	January 2017

Source: 2017 DoD RIO Management Guide, Figure 4-3, p. 46

DAU

Risk Management in the DoD SEP Outline v4.0, 2021

3.2 Technical Tracking

3.2.1 Technical Risk, Issue, and Opportunity Management

- **Technical Risk, Issue, and Opportunity (RIO) Management Process Diagrams**
  - Embed or attach to the SEP the latest (no more than 3 months old) RIO management document including an as-of date.
- **Risk Management Roles**
  - Determine roles, responsibilities, and authorities within the risk management process for the following:
    - Reporting/identifying risks or issues
    - Criteria used to determine whether a "risk" submitted for consideration becomes a risk or not (typically, criteria for likelihood and consequence)
    - Adding/modifying risks
    - Changing likelihood and consequence of a risk
    - Closing/retiring a risk or issue
  - If Risk Review Boards or Risk Management Boards are part of the process, identify the chair and participants and state how often they meet.
  - State how the process will be implemented using the digital ecosystem and digital artifacts, establishing the risk authoritative source of truth (ASoT) while maximizing automated reporting, seamless access, and accuracy of risk status.

3.2.1 Technical Risk, Issue, & Opportunity Management cont.

- **Risk/Issue Management**
  - Risk Tools – Describe the risk management and tracking tools the program office and contractor(s) will use. If the program office and contractor(s) use different risk tools, describe how information will be transferred or integrated without loss. *Note: In general, the same tool should be used. If the contractor's tool is acceptable, the government may opt to use it but must have direct, networked access to the tool.*
  - Technical Risk and Mitigation Planning – Summarize the key engineering, integration, technology, SpENG, and unique SW risks and planned mitigation measures for each risk (DoDI 5000.88, Para 3.4.a.(3)(q)).
  - Risk Reporting – Provide a risk reporting matrix (Figure 3.2-1) or a list of the current system-level technical risks and issues with:
    - As-of date
    - Risk rating
    - Risk statement and consequences, if realized
    - Mitigation activities and expected closure date.

System Safety Risks can also be mapped on the risk cube [*sic*] and reporting matrix in Figure 3.2-1. However, the process for risk burn down shown in Figure 3.2-2 depends on the process to attain acceptance by the System Safety Risk Assessment Authority or mitigation through system safety design order of precedence.

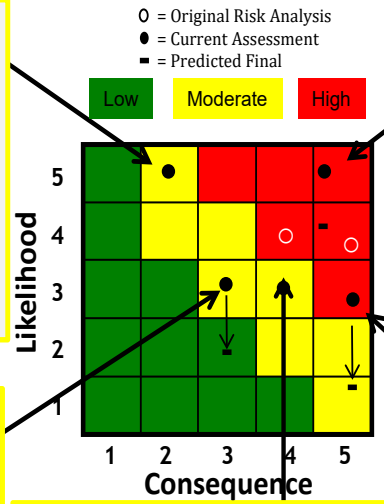
3.2.1 Technical Risk, Issue, & Opportunity Management cont.

Figure 3.2-1 Risk Reporting Matrix
As of [Date] (mandatory) (sample)
{DoD SEP Outline v4.0}

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%

Likelihood scale

- Risk ID #82: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:



- Risk ID #85: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #23: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #45: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #97: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Mitigation Method: (Accept, Avoid, Transfer or Control) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

3.2.1 Technical Risk, Issue, & Opportunity Management cont.

Consequence scale

Level	Cost	Schedule	Performance
5 Critical Impact	10% or greater increase over APB objective values for RDT&E, PAUC, or APUC Cost increase causes program to exceed affordability caps	Schedule slip will require a major schedule rebaselining Precludes program from meeting its APB schedule threshold dates	Degradation precludes system from meeting a KPP or key technical/supportability threshold; will jeopardize program success [2] Unable to meet mission objectives (defined in mission threads, ConOps, OMS/MP)
4 Significant Impact	5% - <10% increase over APB objective values for RDT&E, PAUC, or APUC Costs exceed life cycle ownership cost KSA	Schedule deviations will slip program to within 2 months of approved APB threshold schedule date Schedule slip puts funding at risk Fielding of capability to operational units delayed by more than 6 months[1]	Degradation impairs ability to meet a KSA.[2] Technical design or supportability margin exhausted in key areas Significant performance impact affecting System-of System interdependencies. Work-arounds required to meet mission objectives
3 Moderate Impact	1% - <5% increase over APB objective values for RDT&E, PAUC, or APUC Manageable with PEO or Service assistance	Can meet APB objective schedule dates, but other non-APB key events (e.g., SETRs or other Tier 1 Schedule events) may slip Schedule slip impacts synchronization with interdependent programs by greater than 2 months	Unable to meet lower tier attributes, TPMs, or CTPs Design or supportability margins reduced Minor performance impact affecting System-of System interdependencies. Work-arounds required to achieve mission tasks
2 Minor Impact	Costs that drive unit production cost (e.g., APUC) increase of <1% over budget Cost increase, but can be managed internally	Some schedule slip, but can meet APB objective dates and non-APB key event dates	Reduced technical performance or supportability; can be tolerated with little impact on program objectives Design margins reduced, within trade space [2]
1 Minimal Impact	Minimal impact. Costs expected to meet approved funding levels	Minimal schedule impact	Minimal consequences to meeting technical performance or supportability requirements. Design margins will be met; margin to planned tripwires

Figure 3.2-1 Risk Reporting Matrix as of [Date] (mandatory) (sample) cont. {DoD SEP Outline v4.0}

DAU

3.2.1 Technical Risk, Issue, & Opportunity Management cont.

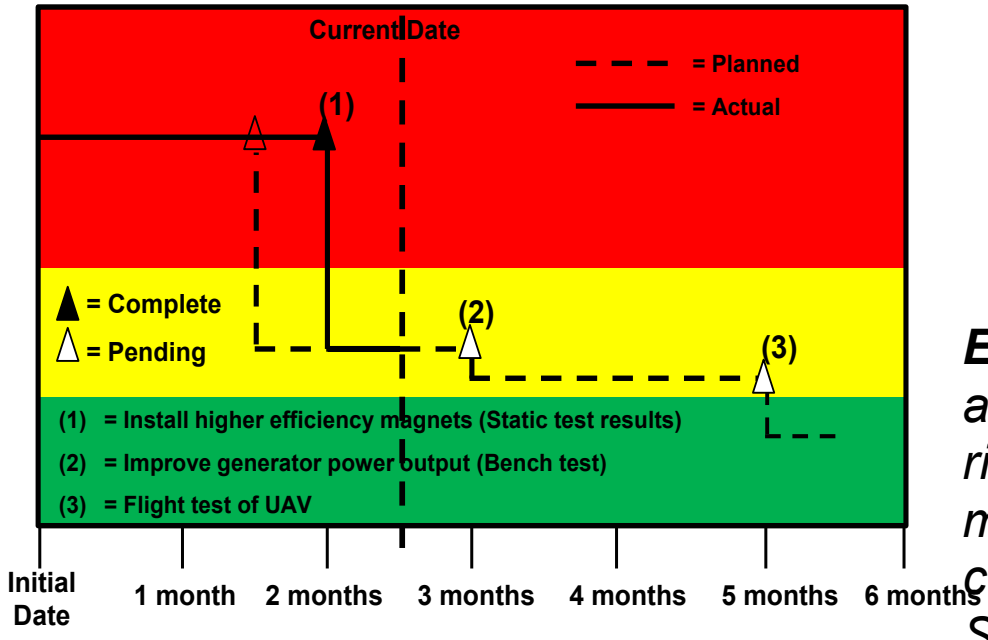


Figure 3.2-2 Risk Burn-Down Plan as of [Date] (mandatory for high risks; others optional) (sample) {DoD SEP Outline v4.0}

Risk Burn-Down

- Describe the program's use of risk burn-down plan to show how the program should implement mitigation activities to control and retire risks. Also discuss how activities are linked to TPMs and to the project schedule for critical tasks. For each high technical risk, provide the risk burn-down plan. (Figure 3.2-2 contains a sample risk burn-down plan.)

Expectation: *Program should use hierarchical boards to address risks and integrates risk systems with contractors. The approach to identify risks is both top-down and bottom-up. Risks related to technology maturation, internal and external integration, modeling, and each design consideration indicated in Table 2.5-1 are considered in risk identification. SEPs submitted for approval contain a current, updated Risk Reporting Matrix and associated Risk Burn-Down plan for high technical risks. Reporting risk artifacts should be auto-generated from within the digital ecosystem at any time depicting the real-time status and should be accessible by all program personnel.*

3.2.1 Technical Risk, Issue, & Opportunity Management cont.

- **Opportunity Management** – Discuss the program's opportunity management plans to create, identify, model, analyze, plan, implement, and track initiatives (including technology investment planning and pollution prevention projects) that can yield improvements in the program's cost, schedule, or performance baseline through reallocation of resources.
  - If applicable, insert a chart or table that depicts the opportunities being pursued, and summarize the cost/benefit analysis and expected closure dates (Table 3.2-1).
  - Address opportunities that would mitigate system safety risks and improve return on investment.

3.2.1 Technical Risk, Issue, & Opportunity Management cont.

Opportunity	Likeli-hood	Cost to Implement	Return on Investment						Program Priority	Management Strategy	Owner	Expected Closure
			Monetary			Schedule	Performance	System Safety Impact				
			RDT&E	Procurement	O&M							
Opportunity 1: Procure Smith rotor blades instead of Jones rotor blades.	Mod	$3.2M			$4M	3-month margin	4% greater lift		#2	Reevaluate; summarize the plan	Mr. Bill Moran	March 2017
Opportunity 2: Summarize the opportunity activity.	Mod	$350K	$25K		$375K				#3	Reject	Ms. Dana Turner	N/A
Opportunity 3: Summarize the opportunity activity.	High	$211K		$0.04M	$3.6M	4 months less long-lead time needed			#1	Summarize the plan to realize the opportunity	Ms. Kim Johnson	January 2017

Table 3.2-1 Opportunity Register (if applicable) (sample)

DAU

Independent Technical Risk Assessment (ITRA)

DoD ITRA Execution Guidance, December 2020

- Implements P.L. 114-328 Sec. 807 enacted in Title 10 U.S.C. Sec. 4272.
- Independent Technical Risk Assessments (ITRAs) will be conducted on all Major Defense Acquisition Programs (MDAPs) prior to Milestone A, Milestone B approval, and any decision to enter into low-rate initial production (LRIP) or full-rate production (FRP).
  - Use *ITRA Framework for Risk Categorization*, USD(R&E), 18 Jun 18
- The ITRA will consider the full spectrum of Technology, Engineering and Integration risk and the potential impacts to cost, schedule and performance. ITRAs provide a view of program technical risk, independent of the program or Component.
  - 8 Areas assessed with 7 Factors, each factor with assessment Criteria; see DTRAM

*DTRAM = Defense Technical Risk Assessment Methodology

- The Under Secretary of Defense for Research and Engineering (USD(R&E)) will conduct or approve ITRAs. This responsibility may be delegated.
- For programs for which an ITRA is conducted, a Technology Readiness Assessment (TRA) will not be conducted.

System Safety Risk Management

- Environmental, Safety, and Occupational Health (ESOH) risks include:
  - Hazardous materials (HAZMAT) use & hazardous waste generation
  - Safety (including explosives safety, radiation, etc.)
  - Human health (chemical, physical, biological, ergonomic, etc.)
  - Environmental & occupational noise
  - Impacts to the environment (air, water, soil, flora, fauna)
- Per DoDI 5000.02 - For ESOH risks, the PM will:
  - Integrate ESOH risk management into the SE process
  - Eliminate ESOH hazards where possible (manage risks that can't be eliminated)
  - Use MIL-STD-882E methodology

System Safety Risk Management (cont'd)

- MIL-STD-882E Safety Order of Precedence:
  - Eliminate hazard through design selection
  - Reduce risk through design alteration
  - Incorporate engineered features or devices
  - Provide warning devices
  - Incorporate signage, procedures, training, and personal protective equipment (PPE)
- Must "accept" residual risk, prior to exposing people, equipment, or the environment. Residual risk acceptance authorities:
  - High risks: Component Acquisition Executive (CAE)
  - Serious risks: Program Executive Officer (PEO)
  - Medium and low risks: Program Manager (PM)
- User representative must be part of this process throughout the lifecycle and will provide formal concurrence prior to all serious and high-risk acceptance decisions.

MIL-STD-882E Severity Table

TABLE I. Severity categories

SEVERITY CATEGORIES		
Description	Severity Category	Mishap Result Criteria
Catastrophic	**1**	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
Critical	**2**	Could result in one or more of the following: permanent partial disability,injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M.
Marginal	**3**	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M.
Negligible	**4**	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K.

Source: MIL-STD-882E 11 May 2012

MIL-STD-882E Probability Table

TABLE II. Probability levels

PROBABILITY LEVELS			
Description	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur often in the life of an item.	Continuously experienced.
Probable	B	Will occur several times in the life of an item.	Will occur frequently.
Occasional	C	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	D	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	F	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.

Source: MIL-STD-882E 11 May 2012

DAU

MIL-STD-882E System Safety Risk Assessment Matrix

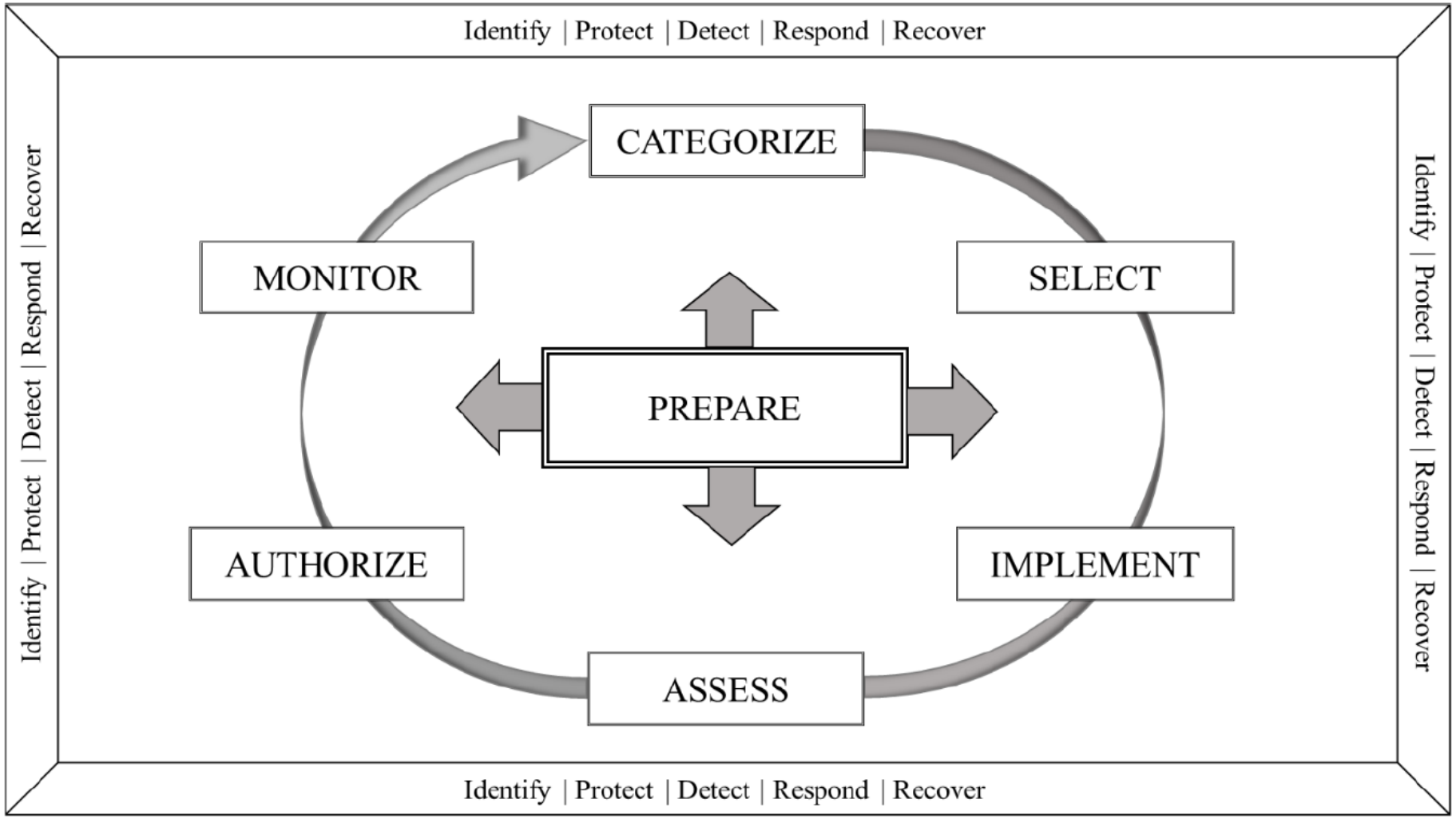
TABLE III. Risk assessment matrix

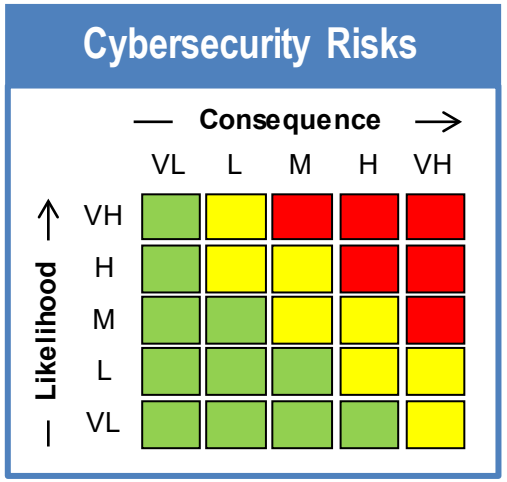
RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Source: MIL-STD-882E 11 May 2012

Cybersecurity - Risk Management Framework (RMF)

Figure 1. RMF Process



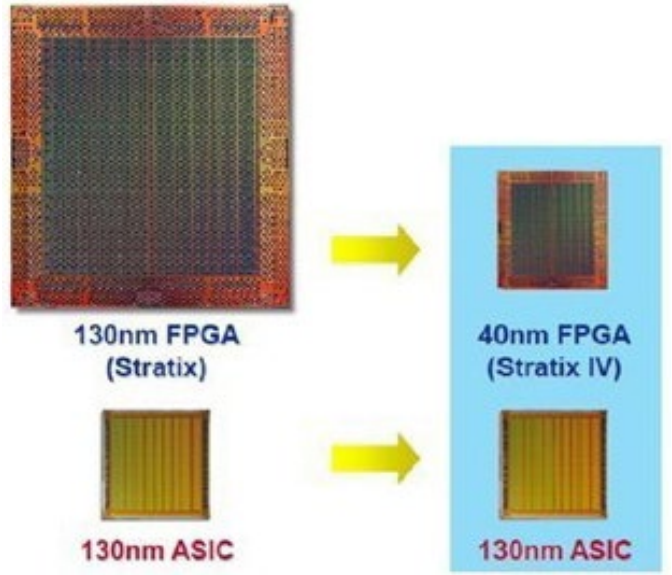


Ref: DoDI 8510.01, 19 Jul 22, for more information

DAU

Supply Chain Risk Management (SCRM) / Trusted Systems & Networks (TSN): Mission Critical Functions (CF) / Components (CC) Identification

- Applies to Information and Communications Technologies (ICT)
- **Criticality Analysis:** process used to identify and prioritize mission critical functions and components via an end-to-end functional decomposition
  - Minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components
- ***Primary concern:*** ASIC*, FPGA** counterfeiting and malware insertion



*ASIC = Application-Specific Integrated Circuit; **FPGA = Field-Programmable Gate Array

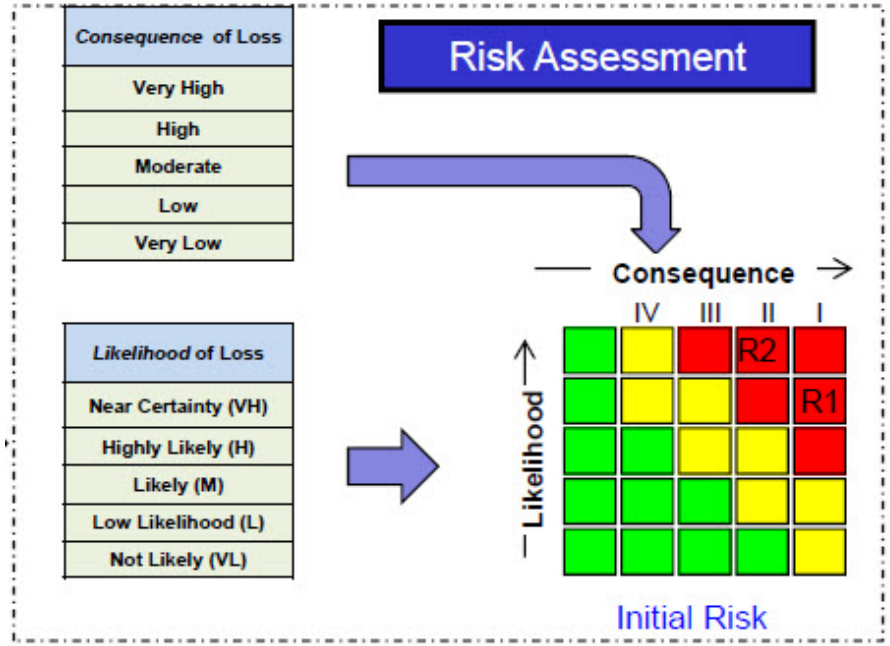
Ref: DoDI 5200.44, Change 3, 15 Oct 18, for more information

CF/CC Risk Assessment / Mitigation

Mission Criticality Assessment

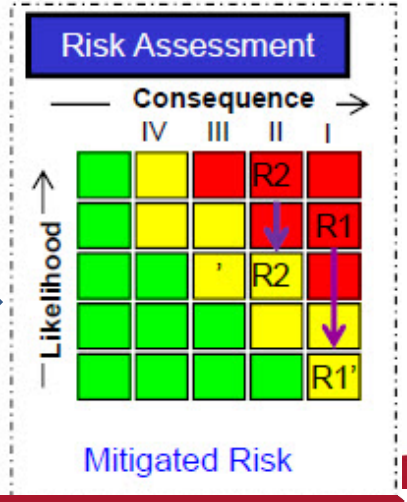
Threat Assessment

Component & Info Vulnerability Assessment



Countermeasures

- SCRM/TSN
  - Trusted Sources
  - Trusted Shipping
  - Bulk Spares Inventory
  - Multiple Suppliers
  - Blind Buys



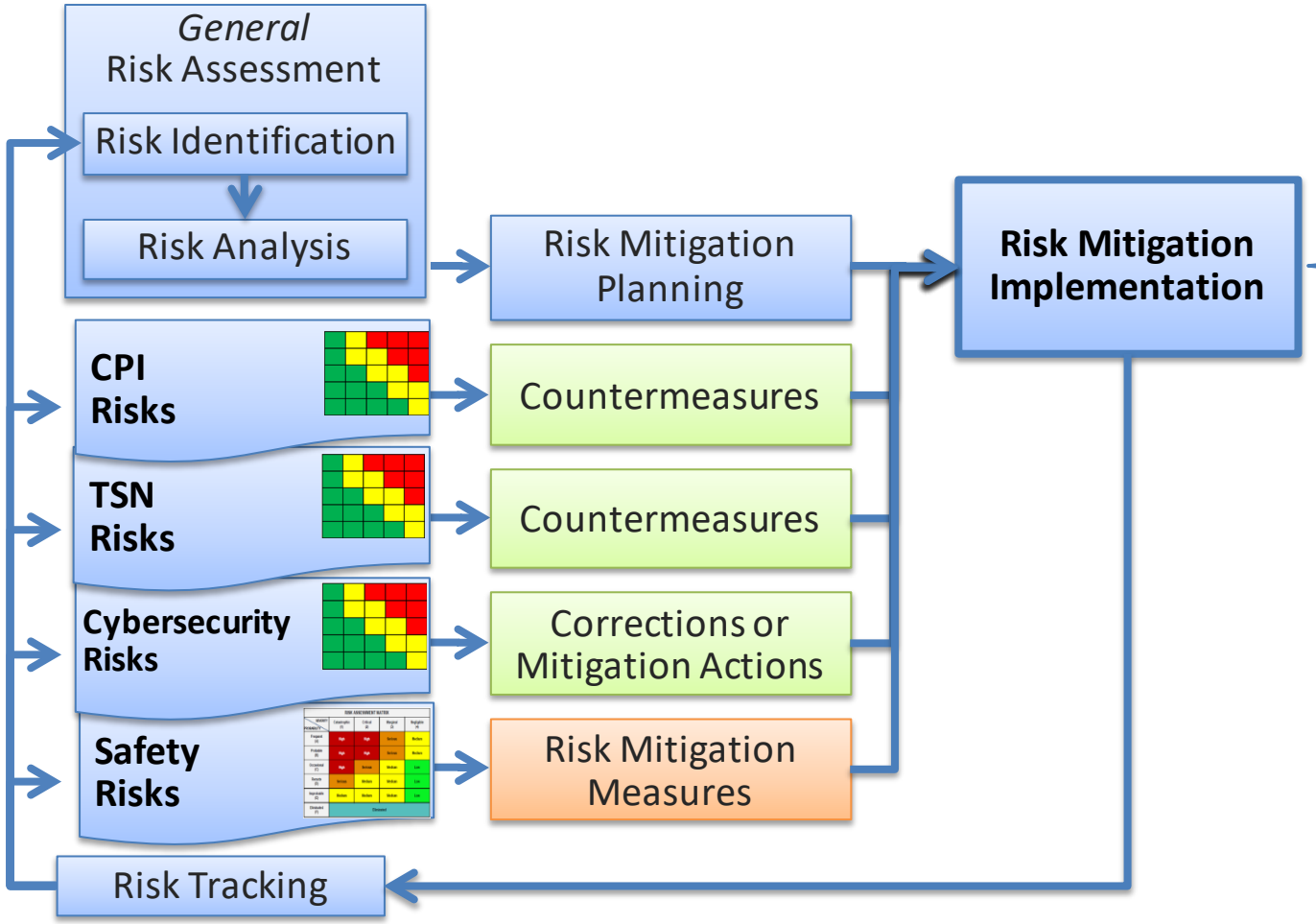
CF/CC (TSN Analysis) Assessment - Example

F-22 Raptors

Criticality Level	Description
Level I Total Mission Failure	Failure that results in total compromise of mission capability
Level II Significant/Unacceptable Degradation	Failure that results in unacceptable compromise of mission capability or significant mission degradation
Level III Partial/Acceptable	Failure that results in partial compromise of mission capability or partial mission degradation
Level IV Negligible	Failure that results in little or no compromise of mission capability

Mission	Critical Function	Logic Bearing Component (ASIC/FPGA)	System Impact Level	Rationale	Countermeasure(s)
Air to Ground Attack	Targeting	Targeting Computer Motherboard ASIC, U25	I	Compromise of the ASIC disables targeting capability.	Purchase U25 from trusted foundry, use secure supply chain.
Air to Ground Attack	Weapon guidance	GPS Computer Motherboard FPGA, IC116	III	Compromise of the FPGA disables GPS guided weapons. Non-GPS guided weapon capability remains.	None recommended due to lower criticality level.
Air Superiority	Target Detection	Radar Transceiver Processor Core PPC, U125	II	Compromise of the radar PPC requires the pilot to "go visual" and use non-radar queued weapon. Redundant PPC designed in the system.	Purchase redundant PPC from alternate supplier (supplier diversity).

Summary – Conduct Integrated Program Risk Management



- All mitigations should be incorporated and prioritized.
- Consider trade-offs against the program constraints.

CPI = Critical Program Information
TSN = Trusted Systems and Networks

The consequences of all risks can be categorized in one of the three categories, i.e., performance, schedule, and cost

Sources for further study

- DoD Risk, Issue, and Opportunity Management Guide, January 2017
- DAU Systems Engineering Brainbook tool Risk Management page
- DAU RIO Management Community of Practice (CoP)
- CACQ 004 Introduction to Risk, Issue, & Opportunity Management Credential
- PMT 0170 Risk Management OLT (8 hrs / 8 CLPs)
- WSM 002 Risk Management Workshop (7 CLPs)
- DAU Webcast: Effectively Evaluating Risk through Factors (source selection)
- Defense Technical Risk Assessment Methodology (DTRAM) v6.3, 30 Sep 20
- DD Engineering Risk Assessments resources; scroll down ERPO page, select “Risk Assessments” tab
- DAU Webcast: Independent Technical Risk Assessment (ITRA) Overview
- MIL-STD-882, System Safety
- DoDI 8510.01, Risk Management Framework for DoD Systems, 19 Jul 22
- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) Change 3, 15 Oct 18