



# **NET-ENABLED COMMAND CAPABILITY Risk Management Plan (RMP)**

**Version 1.0.0  
20 July 2007**

Prepared by:

Net-Enabled Command Capability  
Joint Program Management Office (JPMO)  
P.O. Box 4502  
Arlington, VA 22204-4502

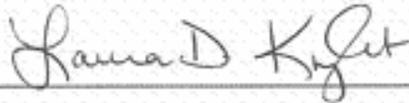
In Collaboration with the NECC Component Program Managers for the Navy, Air Force, Army, Marine Corps, USJFCOM, and DISA.

DISTRIBUTION – Distribution authorized to DoD and DoD Contractors only; for administrative/operational use (11 July 2007). Other requests for this document shall be referred to the NECC Program Management Office.

DESTRUCTION NOTICE – For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

## APPROVAL PAGE

Submitted by:



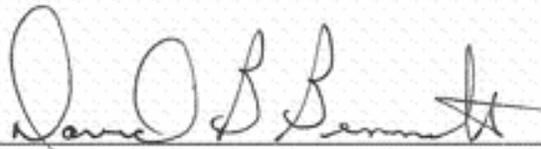
Date:

23 July 2007

LAURA D. KNIGHT

Program Manager,  
Joint Program Management Office (JPMO),  
Net-Enabled Command Capability (NECC)

Concurred by:



Date:

24 Jul 07

DAVID B. BENNETT

Deputy, Program Executive Office,  
Command and Control Capabilities (PEO C2C),  
Defense Information Systems Agency (DISA)

## TABLE OF CONTENTS

<b>APPROVAL PAGE .....</b>	<b>II</b>
<b>1 PURPOSE.....</b>	<b>1</b>
<b>2 SCOPE AND OBJECTIVE .....</b>	<b>1</b>
<b>3 PROGRAM SUMMARY .....</b>	<b>2</b>
3.1 NECC Mission Description .....	2
3.2 Development Schedule .....	2
3.3 Acquisition Strategy .....	3
3.4 Program Management Approach .....	4
<b>4 RISK MANAGEMENT APPROACH.....</b>	<b>5</b>
4.1 Strategy .....	5
4.2 Organization.....	6
4.3 Roles and Responsibilities .....	6
4.3.1 Program Manager (PM) .....	6
4.3.2 Program Management Direction Team.....	7
4.3.3 Risk Management Coordinator .....	7
4.3.4 Component Program Management Offices .....	8
<b>5 RISK MANAGEMENT PROCESS AND PROCEDURES.....</b>	<b>8</b>
5.1 Overview.....	8
5.2 The Risk Management Process Model .....	8
5.3 Risk Planning.....	9
5.4 Risk Identification.....	10
5.5 Risk Analysis .....	10
5.5.1 Purpose.....	10
5.5.2 Risk Reporting Matrix .....	11
5.5.3 Tasks .....	13
5.6 Risk Mitigation Planning.....	14
5.6.1 Purpose.....	14
5.6.2 Tasks .....	14
5.7 Risk Mitigation Plan Implementation.....	15
5.7.1 Purpose.....	15
5.7.2 Tasks .....	15
5.8 Risk Monitoring.....	16
5.8.1 Purpose.....	16
5.8.2 Tasks .....	16
5.8.3 Reporting & Documentation.....	17
5.9 Risk Management Information System .....	18
5.10 Risk Management Training .....	19
<b>APPENDIX A: GLOSSARY.....</b>	<b>20</b>
<b>APPENDIX B: ACRONYMS .....</b>	<b>22</b>
<b>APPENDIX C: REFERENCES.....</b>	<b>24</b>
<b>APPENDIX D: INCREMENT 1 RISKS.....</b>	<b>25</b>

**LIST OF FIGURES**

Figure 1: NECC Program Schedule ..... 2  
Figure 2: JPEO Organizational Structure ..... 5  
Figure 3: NECC Risk Management Process ..... 9  
Figure 4: Risk Reporting Matrix ..... 11  
Figure 5: Levels of Likelihood Criteria ..... 11  
Figure 6: Levels and Types of Consequence Criteria ..... 12  
Figure 7: Risk Analysis and Reporting Illustration ..... 13  
Figure 8: Risk Status Report Format ..... 18  
Figure 9: Risk Management Information Flow ..... 18

## **1 PURPOSE**

The purpose of Net-Enabled Command Capability (NECC) Risk Management Plan (RMP) is to document the NECC Joint Program Management Office's (JPMO's) plan to identify and analyze program risks, develop and implement risk mitigation plans, and track risk issues. The RMP will be used as a guidance document establishing risk management within the program as well as the implementation of a risk control strategy.

## **2 SCOPE AND OBJECTIVE**

Department of Defense (DOD) risk management involves the major activities of risk identification, risk analysis, risk mitigation planning, risk mitigation plan implementation, and risk tracking. Risk management for NECC incorporates these activities and is based on DOD and industry best practices, tailored to meet the needs of the NECC acquisition process. The objective of the NECC RMP is to implement a formal, forward-looking, and continuous risk management process that controls risks through risk mitigation planning and implementation rather than on risk avoidance, transfer, or assumption. This approach is based on the procedures outlined in the DOD Instruction (DODI) 5000.2, "Operation of the Defense Acquisition System," and guidance set forth in the Risk Management Guide for DOD Acquisitions, Sixth Edition.

The NECC JPMO intends to formalize a disciplined risk management process and to implement effective risk mitigation strategies through improved risk management practices. The NECC JPMO will exercise a disciplined risk management strategy throughout the acquisition process and make a determination as to the amount of risk the program will accept as it strives to create value. NECC risk management objectives include:

- Providing visibility into project threats using a structured process
- Identifying development and development dependency threats
- Integrating planning and fielding efforts
- Enabling stakeholders to address shared risks collaboratively
- Focusing management and technical resources on priority risks
- Providing a disciplined approach to program planning
- Providing a reporting and archiving system of risk information
- Controlling potential high-level risks consistent with program cost, schedule, and performance objectives

Anticipated benefits include:

- Improving organizational communication
- Identifying potential risks early as well as mitigating plans for these risks
- Maximizing the use of program resources by targeting high priority risks
- Reducing program costs
- Maintaining accurate schedules
- Achieving expected performance objectives
- Improving business practices

### 3 PROGRAM SUMMARY

#### 3.1 NECC Mission Description

NECC is the DOD’s principal Command and Control (C2) capability that will be accessible in a net-centric environment and will focus on providing the commander with the data and information needed to make timely, effective, and informed decisions. The NECC draws from the C2 community to evolve current and provide new C2 capabilities into a fully integrated, interoperable, collaborative Joint solution. Warfighters can rapidly adapt to changing mission needs by defining and tailoring their information environment and drawing on capabilities that enable the efficient, timely, and effective command of forces and control of engagements.

The NECC program will deliver continuous C2 enhancements to the Warfighter. The program will be founded on a single, net-centric, services-based C2 architecture and provide the decision support infrastructure that will enable the Warfighter to access, display, and understand the information necessary to make efficient, timely, and effective decisions. The Program will be responsive to the Warfighter through loosely coupled capability needs, development, test, and user engagement processes. NECC will leverage existing and evolving C2 capabilities and centers of excellence with its “ABC” commitment to “Adopt-before-Buy, Buy-before-Create”. Key to ABC is adaptation of commercial best practices, architectures and standards for C2. The NECC program will ensure that our C2 capability evolves towards increased net-centricity and Joint mission integration.

#### 3.2 Development Schedule

Figure 1 depicts a high-level schedule of activities for Increment 1 of the NECC program. It shows the program timeline, with subsequent increments shown notionally. Schedules and key events for post-Milestone (MS) B will be developed as necessary in support of MS C information requirements.

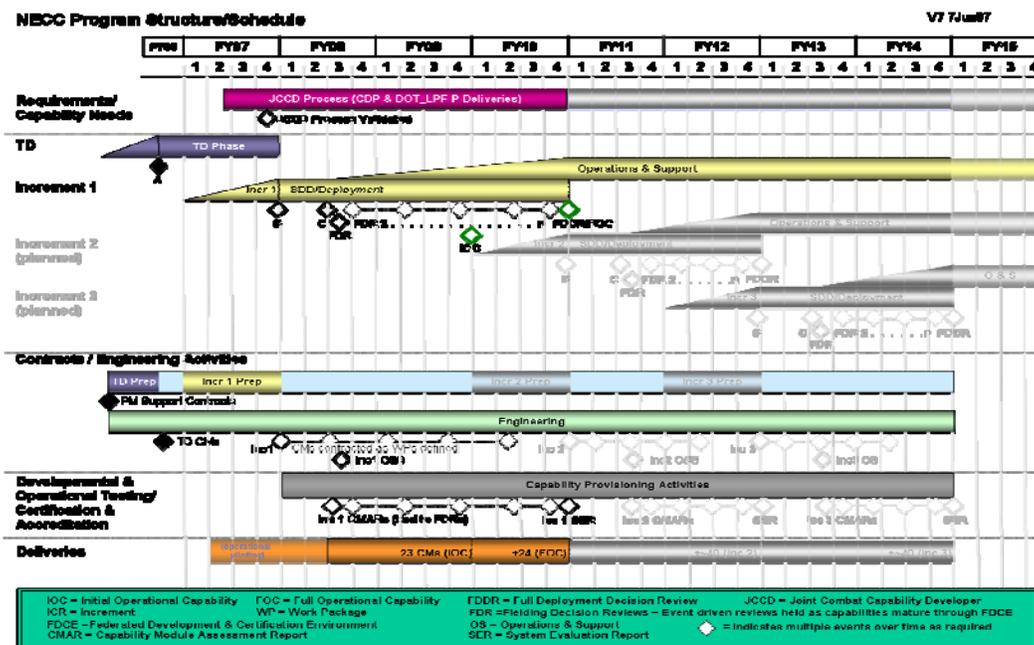


Figure 1: NECC Program Schedule

### 3.3 Acquisition Strategy

The NECC Acquisition Strategy provides the Joint Program Manager (JPM) with a tailored approach to NECC program execution. It is consistent with DOD 5000 guidance, and provides a complete view of the innovative approaches being used to produce NECC. NECC provides the DOD with next-generation C2 capabilities using a Service Oriented Architecture (SOA) on the Global Information Grid (GIG). This strategy lays out a plan to acquire C2 capabilities for the Joint Warfighter to achieve Decision Superiority in engagements, a key tenet of Joint Vision 2020.

NECC is a Joint Acquisition Category (ACAT) 1D Major Defense Acquisition Program and Major Automated Information System. The Milestone Decision Authority (MDA) is the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)/DOD Chief Information Officer (CIO)). The lead component for the Joint program is the Defense Information Systems Agency (DISA). DISA established a Joint Program Executive Office (JPEO) to provide program oversight and a JPMO to manage acquisition requirements, implement the architecture, and perform systems engineering. The Army, Navy, Marine Corps, Air Force, and DISA each established Component Program Management Offices (CPMOs) reporting directly to the JPEO. The CPMOs are responsible for developing NECC C2 capabilities and implementing them within their Component, Service, or Agency (C/S/A). CPMOs produce Capability Modules (CMs) for the program resulting in centralized management with decentralized execution through the Components. The four services and DISA collaborate to develop, refine, and execute program processes and to make decisions as a Joint program.

The Joint Requirements Oversight Council (JROC) assigned NECC requirements oversight to US Joint Forces Command (USJFCOM). USJFCOM established a Joint Combat Capability Development (JCCD) process to manage requirements and provide non-materiel support regarding Doctrine, Organization, Training, Leadership and Education, Personnel, Facilities, and Policy (DOT\_LPF-P).

In March 2006, NECC achieved MS A approval and entered the Technology Development (TD) phase. The MDA directed key exit criteria to be accomplished during the TD phase. TD phase Capability Provisioning Activities (CPAS) are designed to demonstrate the technology required for the System Development and Demonstration (SDD) phase. A subset of the CMs under development in the TD phase is used in CPAS events to demonstrate that C2 missions can be conducted equal to or better than current capabilities for disconnected operations. USJFCOM is demonstrating the JCCD process in conjunction with the TD phase CPAS.

The program is resolving technology shortfalls for SDD development and demonstrating the ability to execute the NECC process for the SDD phase. A key component of this is demonstrating a Federated Development and Certification Environment (FDCE) maturity. CPAS activities use the FDCE, which is the virtual environment where developers, testers, certifiers, and users collaboratively interact with NECC capabilities as they are created and implemented on the GIG. The program established an approach to security and interoperability in accordance with policy by using the FDCE.

The NECC Acquisition Strategy for the SDD phase is to build net-centric services as CMs, not as large, completely integrated software system. CMs are small, militarily useful pieces of software, loosely coupled via the SOA and resident on the GIG. A key concept behind NECC is to build capabilities and deliver CMs to the Warfighter, as they are ready, not to wait for major milestones for a complete software release. The individual nature of CMs and the planned

responsiveness to the Warfighter requires agility and flexibility in NECC's systems engineering, development, contracting, testing, funding, and acquisition processes, which are all described in the Acquisition Strategy. Rapid delivery results in having multiple CMs in concurrent stages of development, operations, or sustainment within an increment, which changes the nature of the program's Milestone Decisions and funding requirements. The result is a net-centric set of services rapidly provided to Warfighters, which gives them the capabilities they need to achieve and sustain Decision Superiority and accomplish their missions.

### **3.4 Program Management Approach**

NECC is not the effort of a single military component, but is a collaborative effort across the C2 spectrum. DISA is the lead component for managing and directing the contributions of the others, but all the components will participate in shaping the new architecture, especially the military services. Each Service has set up its own CPMO in support of the NECC and has placed that office under the management control of the Command and Control Capability (C2C) Program Executive Office (PEO), established by DISA as the JPEO (see Figure 2). The PEO C2C is the single Joint office for management of the NECC program. USJFCOM has been designated as the Operational Sponsor and will act as the end-user representative during the design and development of Capability Development Packages (CDPs). In addition, the NECC Risk Management Coordinator (RMC) has been tasked with coordinating risk management activities and is responsible for organizing, reporting, providing guidance on, and making recommendations in support of risk management activities.

The NECC JPMO has established the Program Management Direction Team (PMDT) to manage and direct the cost, schedule, performance, issue resolution and risk mitigation activities of the NECC as chartered by the C2C PEO. Members of the PMDT include the CPMO management and chief engineer representatives, CM developer organizations, subordinate top-level working group leads, Working Integrated Product Team (WIPT) leads, and an USJFCOM representative. The PMDT is empowered by the PEO to make decisions that are in the best interest of the NECC; resolvable issues and problems, and ensure requirements are met. The PMDT then forwards any unresolved issues to the PEO for resolution. Direction is provided following the program fundamentals. The PMDT charters working groups and tasks those groups to support effective decision-making and issue resolution.

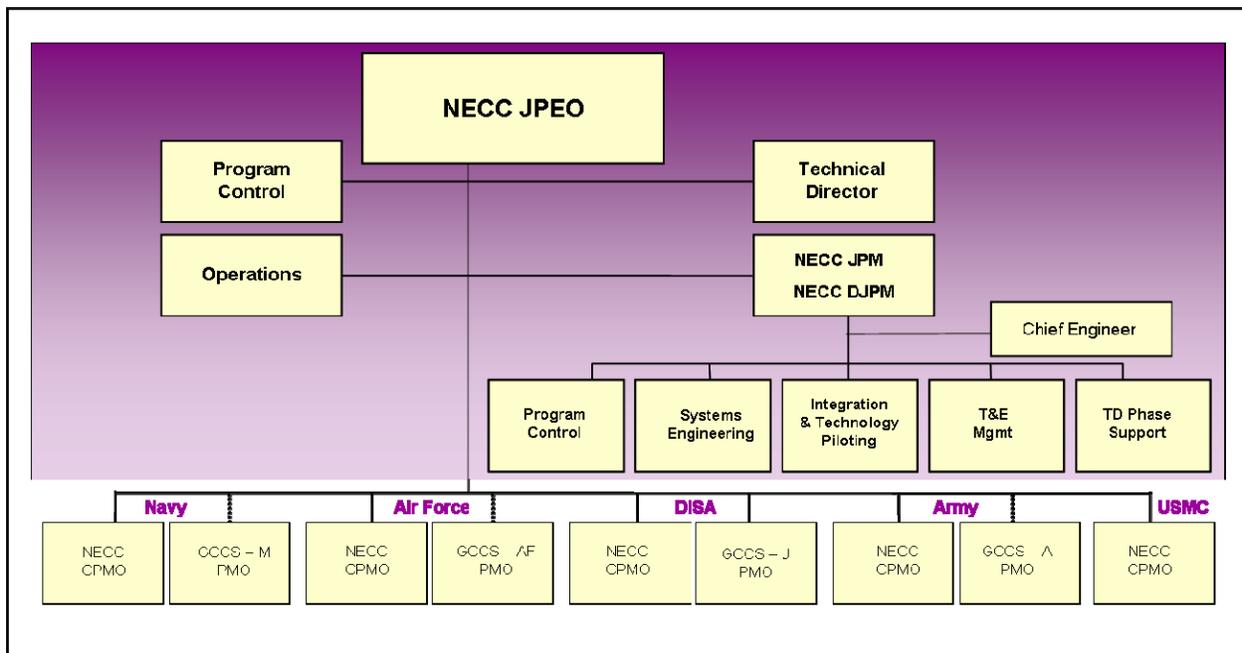


Figure 2: JPEO Organizational Structure

## 4 RISK MANAGEMENT APPROACH

A risk is a situation, event, or condition that could potentially prevent or delay the achievement of program objectives. Attributes of a risk include:

- Likelihood of risk-realization
- Potential impact
- Risk timeframe (estimates of time to risk-realization, time from risk-realization to impact, and impact duration)
- Organization controlling the source of the risk (external, distinct levels of internal controls)

Risk management is a systematic, iterative process that involves identifying, analyzing, and responding to risks. For the risk management process to work effectively and efficiently, the process must be formally documented and communicated to all stakeholders; and risk identification must be considered in all program elements. For the NECC program, risk management activities are in place, implementing risk control strategies across all program disciplines. The intent is to use continuous and effective risk management throughout the JPMO to support program objectives. This involves conducting formal risk assessments, integrating formal risk management practices, and continuing to implement the risk management strategy.

### 4.1 Strategy

The NECC risk management strategy provides *centralized* risk management identification, guidance, and system review throughout the acquisition process with *decentralized* risk planning, assessment, handling, and monitoring of the individual risk events. The basic risk management approach is to first identify high impact risk events and to then assess existing actions or recommend new actions to control the risk events in order to avoid serious program impacts.

The risk management approach is intended to accommodate the possibility of failures in all program elements, including:

Cost: Uncertainty of having sufficient financial resources to address risks if they should materialize.

Schedule: Uncertainty in achieving schedule milestones if risks should materialize.

Performance: Uncertainty in achieving the threshold or objective capabilities.

Development: Uncertainty of the individual mission application to achieve or satisfy functional and technical requirements.

Integration: Uncertainty of system integrators to produce an operable capability.

Technology: Uncertainty associated with the dependence of NECC on external technologies required for its implementation.

Security: Uncertainty associated with security vulnerabilities.

Supportability: Uncertainty of having sufficient support resources available such as appropriate personnel with the required skills and training; facilities for development, testing, and integration; documentation to support users, infrastructure to support the mission applications, and a maintenance plan for the infrastructure supporting the mission applications.

Test Certification/Accreditation: Uncertainty associated with a capabilities' ability to satisfy Federated testing, certification, and accreditation criteria.

Environmental Safety and Occupational Health (ESOH): Uncertainty associated with being able to comply with all federal, state and local, and where necessary, international environmental policies.

The risk management process will assess planned activities to identify possible issues that could cause significant program impact. All identified risks will be assessed as to their likelihood of realization, and the extent of their impact should they be realized. Mitigation plans will be developed for all possible risk events that result in an elevated risk rating. Mitigation plans will be continuously tracked, monitored, and reported on in order to reduce or eliminate the overall program risk.

## **4.2 Organization**

The NECC risk management review process will operate using the PEO C2C management structure detailed in Section 3.4. The PMDT is responsible for implementing the NECC program's risk management process, and provides the forum for proposing new risk areas for analysis and mitigation. The RMC tracks and monitors all identified program risks, and periodically provides reports and recommendations to the PMDT for management consideration and mitigation.

## **4.3 Roles and Responsibilities**

### **4.3.1 Program Manager (PM)**

- Oversee the program's risk management activities
- Co-chair the PMDT
- Ensure resources are available to support risk management

- Plan, organize, direct, and control risk management in compliance with applicable DOD documents
- Approve risk mitigation plans
- Identify top project risks to Project Sponsor(s) and stakeholders
- Review project risks identified and assessed by the PMDT
- Monitor project risk status, mitigation efforts, and contingency plans
- Report risk status, trend analysis, and success of mitigation efforts of the program's top risks to the PEO and stakeholders

#### **4.3.2 Program Management Direction Team**

- Co-chaired by the Program Manager and the Chief Engineer
- Ensure a risk management program is in place
- Delegate and guide risk assessment efforts
- Periodically review project risk management reports (stand-alone or integral to project management) from the RMC
- Periodically provide project risk management general direction and specific decisions (stand-alone or integral to project management) to RMC
- Validate risk assessments, risk mitigation plans, and monitoring requirements
- Identify new project risks
- Identify, report, and assist in responding to risks relating to the end-users' knowledge of the project's products; willingness to use the project's products; and, the ability to make the changes necessary for the project's success including:
  - Requirements validation and analysis
  - Communication to stakeholders and customers
  - Training and documentation to operators and end-users
- Approve risk response strategies and plans (mitigation and contingency plans) for top program risks
- Identify resources required and available for risk mitigation plans
- Escalate the risks to higher levels, when this is deemed as the appropriate action
- Evaluate the effectiveness of the NECC risk management program

#### **4.3.3 Risk Management Coordinator**

- Maintain and execute the RMP
- Track and monitor program risks
- Maintain the Risk Management Information System (RMIS)
- Monitor program compliance within DOD risk management guidelines
- Plan and coordinate risk management training as required
- Coordinate risk management activities with the PM and the PMDT
- Develop and update project risk management framework and plans
- Analyze project risks and provide results to the PM and PMDT.
- Recommend to the PMDT delegation of responsibility for individual risks to program staff members as appropriate
- Recommend to the PMDT risk response strategies and plans (mitigation and contingency plans)
- Review project risk management progress periodically
- Review re-assessment of project risks, mitigation efforts, and contingency planning

- Prepare reports on risk status, trend analysis, and success of mitigation efforts of the program's top risks
- Assist in developing and implementing risk response options and mitigation strategies for identified risks
- Maintain oversight of risk management activities to include providing lessons learned and best practices
- Coordinate risk management activities with other program areas, as required
- Integrate risk management activities across the program
- Enable anonymous risk entries using Risk Assessment Forms
- Coordinate risk issues with the CPMOs

#### **4.3.4 Component Program Management Offices**

- Support risk management activities
- Assess Service-level risks and elevate to the JPMO as necessary
- Coordinate risk findings and decisions within the Components
- Identify and provide resources for implementing risk mitigation plans
- Provide measures and recommendations in support of risk control
- Identify and report to the RMC risks related to the following:
  - Data architecture
  - Network and security
  - Technical requirements management
  - Configuration management
  - Verification and validation
  - Development and testing
  - Operations and maintenance
  - Cost, schedule, and performance
- Assist the RMC as required

## **5 RISK MANAGEMENT PROCESS AND PROCEDURES**

### **5.1 Overview**

Risk management is a continuous process that is accomplished throughout the life cycle of a system. It is an organized methodology for continuously identifying and measuring the unknowns; developing mitigation options; selecting, planning, and implementing appropriate risk mitigations; and tracking the implementation to ensure successful risk reduction. Effective risk management depends on risk management planning; early identification and analyses of risks; early implementation of corrective actions; continuous monitoring and reassessment; and communication, documentation, and coordination.

### **5.2 The Risk Management Process Model**

The risk management process model (see Figure 3) includes the following key activities, performed on a continuous basis:

- Risk Identification
- Risk Analysis
- Risk Mitigation Planning/Implementation
- Risk Monitoring

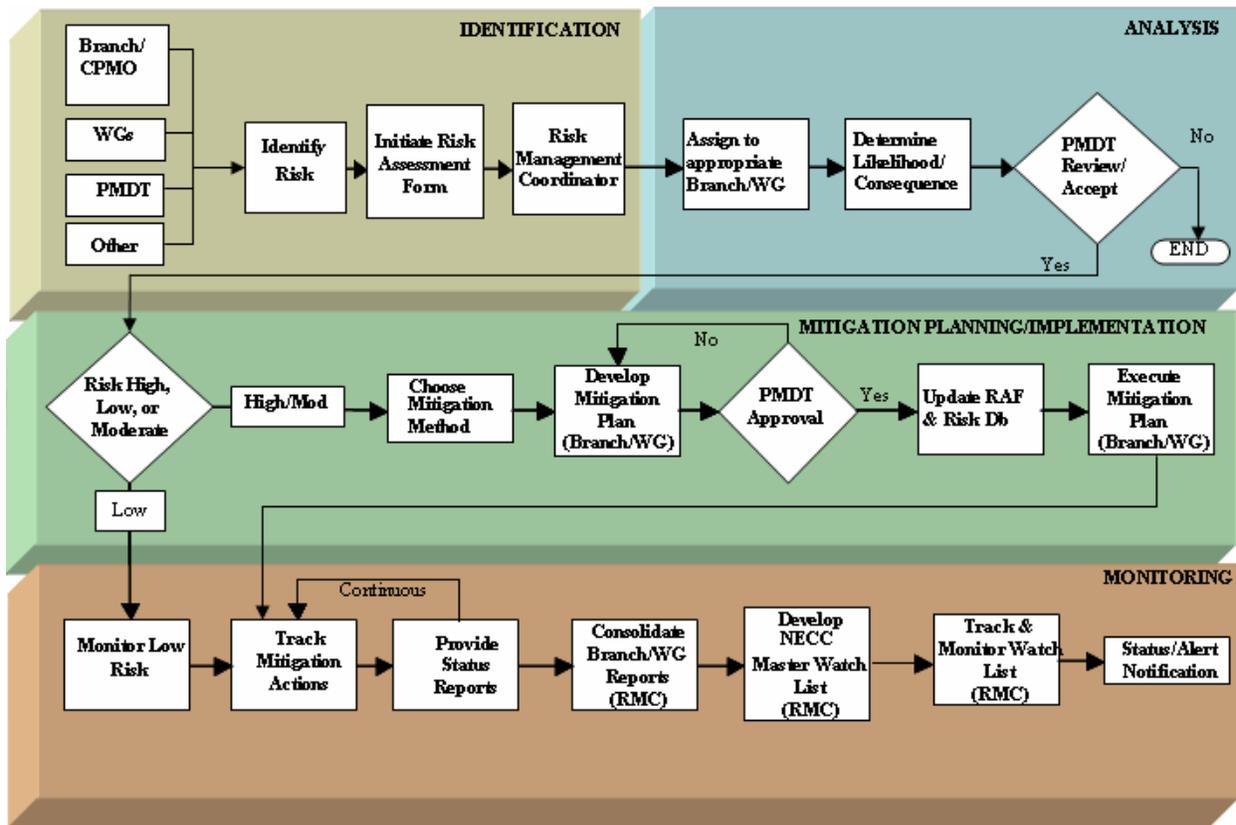


Figure 3: NECC Risk Management Process

### 5.3 Risk Planning

Risk planning is an integral part of the normal program planning and management effort and consists of the up-front activities necessary to execute a successful risk management program. NECC's risk planning involves developing and implementing procedures to ensure an effective risk management program. It also assigns responsibilities for specific risk management actions and establishes risk reporting and documentation requirements. Risk planning is iterative by nature and the plan will be revised as the risk management process is executed and evaluated, as required to support another phase of the acquisition, or as directed by the NECC PM. Updates are based on program/schedule changes and evaluations by the JPMO of how well risk management has been implemented. Criteria for the evaluations include the following:

- **Planning.** Has the program effectively planned for risk management? Has it been systematic in application? Does it have a method to identify and track risk areas against critical path items and Work Package elements? Are risk-handling and corrective action plans developed?
- **Assessment.** Has the program considered future issues, not just current problems?
- **Technical Focus.** What are the current technical risks?
- **Documentation.** Have all aspects of risk management been recorded? Has a database system been established to store archived documents and was it used effectively?

- Continuity. Were risk assessments made throughout the development phase? Have follow-up actions been evaluated and revised accordingly? Have resources been focused on priority risks?

This RMP documents the risk management process, and serves as the basis for all subsequent detailed risk planning.

## 5.4 Risk Identification

Risk identification defines the set of events that could have an adverse impact on a project's cost, schedule, or technical performance requirements. The objectives of risk identification are to enumerate known project risks and identify risks not immediately evident to the project team. Risk identification occurs continuously throughout the program's life cycle. All identified risks originate using the Risk Assessment Form, which is used to understand the details of the risk as well as mitigation and contingency plans. Risks can be identified at key programmatic meetings, reviews of program and external documents, and PMDT meetings. Potential risk candidates can be identified and inserted into the Risk Management database at any time, and any stakeholder within the NECC community can identify a risk. Risk can be both internal and external to the program.

Identified risks will be described and communicated to management in the form of risk statements. A risk statement should provide sufficient clarity and descriptive information so that the risk's occurrence probability and area(s) of impact can be assessed. Risk statements should contain two components: (1) a statement of the present condition, and (2) the associated risk event(s). The goal of a risk statement is to develop and document clear, concise, easily understood statements. Consider these questions when writing a risk statement:

1. Does it come from a known FACT? All risks come from an existing fact, condition, or decision.
2. Is it clear and concise?
3. Will most project members understand it?
4. Will the statement be understandable in six months or a year?
5. Is there a clear event or source of concern or worry?
6. Is the consequence(s) clear and understandable?
7. Is there only ONE potential event or condition? If there is more than one event or condition, then you have more than one risk.

The Condition-If-Then format is recommended for writing risk statements. It provides a more complete picture of the risk. This format can be described as follows: *Starting from a CONDITION or FACT; IF an event occurs; THEN there is a consequence(s).*

## 5.5 Risk Analysis

### 5.5.1 Purpose

The intent of risk analysis is to answer the question, "How big is the risk?" by:

- Considering the likelihood of the root cause occurrence
- Identifying the possible consequences in terms of performance, schedule, and cost
- Identifying the risk level using the Risk Reporting Matrix shown in Figure 4.

### 5.5.2 Risk Reporting Matrix

Each undesirable event that might affect the success of the program (performance, schedule, and cost) should be identified and assessed as to the likelihood and consequence of occurrence. A standard format for evaluation and reporting of program risk assessment findings facilitates common understanding of program risks at all levels of management. The Risk Reporting Matrix below (Figure 4) is typically used to determine the level of risks identified within a program. The level of risk for each root cause is reported as low (green), moderate (yellow), or high (red).

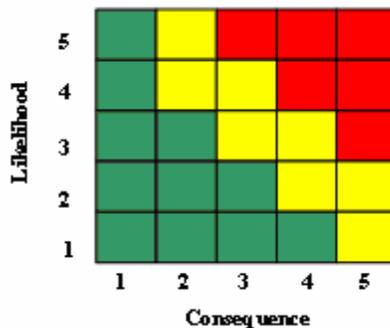


Figure 4: Risk Reporting Matrix

The level of likelihood of each root cause is established using specified criteria (Figure 5). For example, if the root cause has an estimated 50 percent probability of occurring, the corresponding likelihood is Level 3.

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

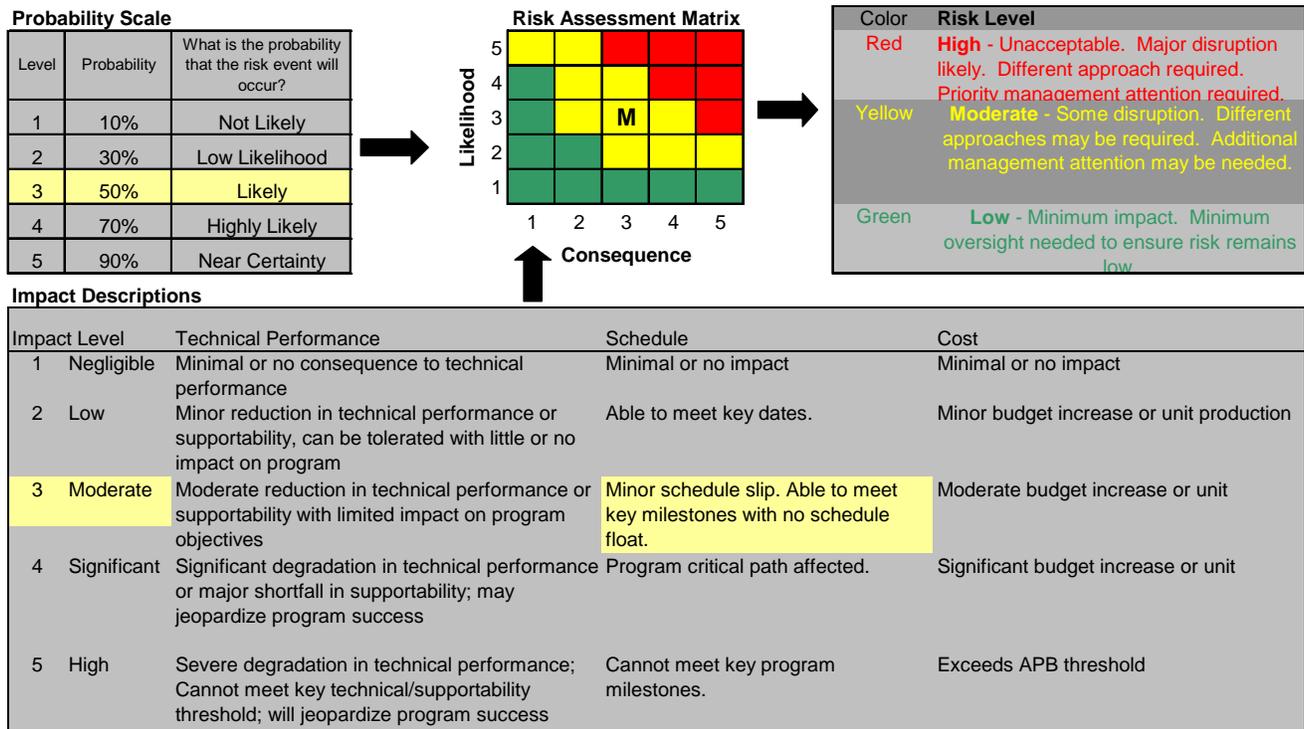
Figure 5: Levels of Likelihood Criteria

The level and type of consequences of each risk are established using the criteria in Figure 6. Continuing with the prior example of a root cause with a 50 percent probability of occurring, if that same root cause has no impact on performance or cost, but may likely result in a minor schedule slippage that will not impact a key milestone, then the corresponding consequence is a Level 3 for this risk. For clarity it is also classified as a *schedule* risk since its root cause is schedule related.

<i>Consequences</i>	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.	Minor budget increase or unit production cost increases.
	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.	Moderate budget increase or unit production cost increase
	4	Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success	Program critical path affected.	Significant budget increase or unit production cost increase
	5	Severe degradation in technical performance; Cannot meet KPP or key technical/supportability threshold; will jeopardize program success	Cannot meet key program milestones.	Exceeds APB threshold

**Figure 6: Levels and Types of Consequence Criteria**

The results for each risk are then plotted in the corresponding single square on the Risk Reporting Matrix. In this example, since the level of likelihood and consequence were both “3,” the corresponding schedule risk is reported as “yellow,” (see Figure 7).



**Figure 7: Risk Analysis and Reporting Illustration**

### 5.5.3 Tasks

Risk analysis is the activity of examining each identified risk to refine the description of the risk, isolate the cause, determine the effects, and aid in setting risk mitigation priorities. It refines each risk in terms of its likelihood, consequence, and relationship to other risk areas or processes. Analysis begins with a detailed study of the risks that have been identified. The objective is to gather enough information about future risks to judge the root causes, the likelihood, and the consequences if the risk occurs. The frequently used term “risk assessment” includes the distinct activities of risk identification and risk analysis.

Risk analysis sequence of tasks includes:

- Develop probability and consequence scales by allocating consequence thresholds against the Work Breakdown Structure (WBS) or other breakout
- Assign a probability of occurrence to each risk using the criteria presented in Section 5.5.2 (Figure 5)
- Determine consequence in terms of performance (P), schedule (S), and/or cost (C) impact using the criteria presented in Section 5.5.2 (Figure 6)
- Document the results in the program risk database

Note: Risk analysis is a snapshot-in-time and may change significantly during the program. Risk analyses must be periodically re-accomplished to ensure the analysis remains current.

NECC will use a WBS approach in which risks are identified, assessed, and tracked for individual WBS elements at their respective levels (primarily for impact on cost and schedule performance) and for their resulting effect on the overall product. Since DOD programs are generally established around the WBS, each product’s associated costs and schedule can be readily baselined, and its risk consequence can be measured as a deviation against this baseline.

Taking the WBS to sequentially lower levels will help assure all required products are identified, along with allocations for cost and schedule performance (as well as operational performance) goals.

Integration of performance, schedule, and cost analyses into a single process supports a program that starts with well-defined requirements, builds upon a solid technical foundation, develops a realistic program schedule, and documents the resources needed in the program cost estimates. Program root cause identification and analysis integrates the technical performance assessment, schedule assessment, and cost estimates using established risk evaluation techniques. Each of these risk categories (cost, schedule, and performance) has activities of primary responsibility, but provides inputs and support from the other two risk categories. This helps to keep the process integrated and to ensure the consistency throughout the program lifecycle.

## **5.6 Risk Mitigation Planning**

### **5.6.1 Purpose**

The intent of risk mitigation planning is to answer the question “*What is the program approach for addressing this potential unfavorable consequence?*” One or more of these mitigation options may apply:

- Controlling the cause or consequence
- Avoiding risk by eliminating the root cause and/or the consequence
- Transferring the risk
- Assuming the level of risk and continuing on the current program plan

Risk mitigation planning is the activity that identifies, evaluates, and selects options to set risk at acceptable levels given program constraints and objectives. Risk mitigation planning is intended to enable program success. It includes the specifics of what should be done, when it should be accomplished, who is responsible, and the resources required to implement the Risk Mitigation Plan. While the preferred method is to control the risk through mitigation and planning, the most appropriate approach is selected from the mitigation options listed above and documented in a Risk Mitigation Plan.

The level of detail depends on the program Life Cycle phase and the nature of the need to be addressed. However, there must be enough detail to allow a general estimate of the effort required and technological capabilities needed based on system complexity.

### **5.6.2 Tasks**

For each root cause or risk, the type of mitigation must be determined and the details of the mitigation described.

Once alternatives have been analyzed, the selected mitigation option should be incorporated into program planning, either in existing program plans or documented separately as a Risk Mitigation Plan (not to be confused with the risk management plan). The Risk Mitigation Plan needs to be realistic, achievable, measurable, documented, and address the following topics:

- A descriptive title for the identified risk
- The date of the plan
- The point of contact responsible for controlling the identified root cause

- A short description of the risk (including a summary of the performance, schedule, and resource impacts; likelihood of occurrence; consequence; and whether the risk is within the control of the program)
- Why the risk exists (root causes leading to the risk)
- The options for mitigation (possible alternatives to alleviate the risk)
- Definition of events and activities intended to reduce the risk, success criteria for each plan event, and subsequent “risk level if successful” values
- Risk status (discuss briefly)
- The fallback approach (describe the approach and expected decision date for considering implementation)
- A management recommendation (whether budget or time is to be allocated, and whether or not the risk mitigation is incorporated in the estimate at completion or in other program plans)
- Appropriate approval levels (Integrated Product Team (IPT) leader, higher-level Product Manager, Systems Engineer, and PM)
- Identified resource needs
- Determine if current work package funding is adequate to complete all the tasks (including risk mitigation plans) within the respective work packages

## **5.7 Risk Mitigation Plan Implementation**

### **5.7.1 Purpose**

The intent of risk mitigation (plan) execution is to ensure successful risk mitigation occurs. It answers the question “*How can the planned risk mitigation be implemented?*” It:

- Determines what planning, budget, and requirements and contractual changes are needed
- Provides a coordination vehicle with management and other stakeholders
- Directs the teams to execute the defined and approved risk mitigation plans
- Outlines the risk reporting requirements for on-going monitoring
- Documents the change history

### **5.7.2 Tasks**

Risk assessment (identification and analysis) is accomplished by risk category. Each risk category (e.g., performance, schedule, and cost) includes a core set of assessment tasks and is related to the other two categories. These interrelationships require supportive analysis among areas to ensure the integration of the assessment. Implementing risk mitigation should also be accomplished by risk category, and it is important for this process to be worked through the JPMO structure, requiring the Branches/WGs at each WBS level to scrub and endorse the risk mitigations of lower levels. It is important to mitigate risk where possible before passing it up to the next WBS level. In addition, each Branch/WG must communicate potential cost or schedule growth to all levels of management. It is imperative that the Chief Engineer and PM understand and approve the mitigation plan and examine the plan in terms of secondary, unforeseen impacts to other elements of the program. As part of this effort, the Branches/WGs should ensure effective mitigation plans are implemented and ongoing results of the risk management process are formally documented and briefed, as appropriate, during program and technical reviews.

When determining that it may be appropriate to lower the consequence of a risk, careful consideration should be given to the justification for doing so. This includes identifying exactly what about the risk has changed between the time of the original consequence assessment and the current risk state to justify such a reassessment.

When feasible and deemed necessary by the JPMO, cost and/or schedule metrics will be established for monitoring the status of risk mitigation actions. Metrics should be carefully selected to ensure they accurately relate the status of the mitigation actions.

## **5.8 Risk Monitoring**

### **5.8.1 Purpose**

The intent of risk tracking is to ensure successful risk mitigation. It answers the question “*How are things going?*” by:

- Communicating risks to all affected stakeholders
- Monitoring risk mitigation plans
- Reviewing regular status updates
- Displaying risk management dynamics by tracking risk status within the Risk Reporting Matrix (see Section 5.5.2)
- Alerting management as to when risk mitigation plans should be implemented or adjusted

Risk monitoring activities are integral to good program management. At a top level, periodic program management reviews and technical reviews provide much of the information used to identify any performance, schedule, readiness, and cost barriers to meeting program objectives and milestones.

NECC risk monitoring of documents may include: program metrics, technical reports, earned value reports, watch lists, schedule performance reports, technical review minutes/reports, and critical risk processes reports.

An event's likelihood and consequences may change as the acquisition process proceeds and updated information becomes available. Therefore, throughout the program, the JPMO will reevaluate known risks on a periodic basis and examine the program for new root causes.

### **5.8.2 Tasks**

Risk monitoring is the activity of systematically tracking and evaluating the performance of risk mitigation actions against established metrics throughout the acquisition process. It feeds information back into the other risk activities of identification, analysis, mitigation planning, and mitigation plan implementation as shown in Figure 3.

The key to the tracking activity is to establish a management indicator system over the entire program. The JPMO uses this indicator system to evaluate the status of the program throughout the life cycle. It is designed to provide early warning when the likelihood of occurrence or the severity of consequence exceeds pre-established thresholds/limits or is trending toward exceeding pre-set thresholds/limits so timely management actions to mitigate these problems can be taken.

The JPMO will re-examine risk assessments and risk mitigation approaches concurrently. As the system design matures, more information becomes available to assess the degree of risk inherent in the effort. If the risk changes significantly, the risk mitigation approaches will be adjusted

accordingly. If the risks are found to be lower than previously assessed, then specific risk mitigation actions may be reduced or canceled and the funds reprogrammed for other uses. If they are higher, or new root causes are found, appropriate risk mitigation efforts will be implemented.

The PMDT, in its capacity as a risk management board, will periodically review risk mitigation actions for their effect on the risk issue. Mitigation plans may be modified depending on the specific need to lower the risk or to re-direct resources to more critical risk areas. Risk items may be opened, closed, mitigated, monitored, or retired by the PMDT.

### **5.8.3 Reporting & Documentation**

The purpose of risk reporting is to ensure the JPMO receives all necessary information to make timely and effective decisions. This allows for coordination of actions by the risk team, allocation of resources, and a consistent, disciplined approach. The primary goal of risk reporting is to provide the JPMO with an effective early warning of developing risk.

Risk documentation is the recording, maintaining, and reporting of identifications, analyses, mitigation planning and implementation, and tracking results. Risk tracking should be done as part of technical reviews, risk review board meetings, or periodic program reviews. Documentation includes all plans and reports for the JPMO and decision authorities. It also includes reporting forms that may be internal to the program office. This is consolidated in the Risk Mitigation Plan.

Risk reporting should present standard likelihood and consequence screening criteria, as well as the Risk Reporting Matrix presented in Section 5.5.2. The details regarding consequences for cost, schedule, and performance should be documented in each Risk Mitigation Plan. The plotted position on the Risk Reporting Matrix should show the current assessment of the risk's likelihood and the estimated severity of its effect on the program if mitigation fails. As risk mitigation succeeds in a program, a yellow or red risk's position on the Risk Reporting Matrix will migrate in successive assessments from its current location toward the green. Each risk description should include three key elements (Figure 8 provides an example):

- A brief description, including both the title and type (P, S, or C), of the risk
- A brief description of the risk root causal factor(s)
- The planned mitigations, along with critical dates (risk reduction milestones), that address the root cause(s) and effect(s)

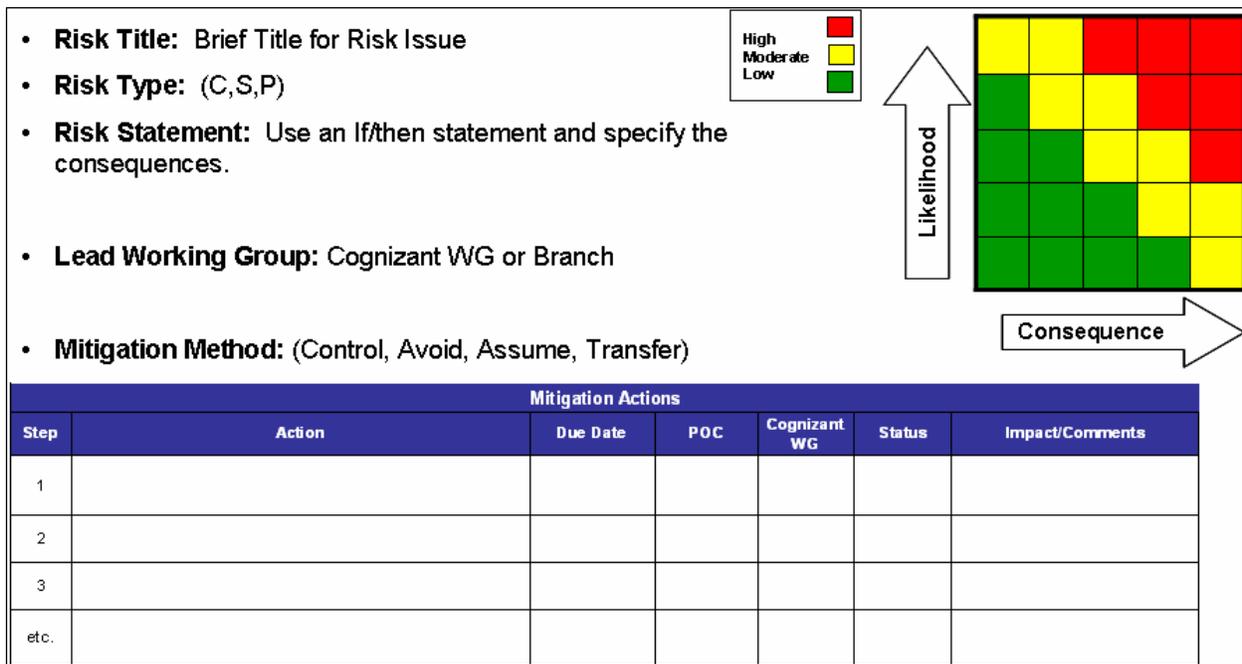


Figure 8: Risk Status Report Format

### 5.9 Risk Management Information System

The RMIS is a software application that stores and sorts risks and generates risk management reports. The purpose of the RMIS is to provide a tool for tracking, monitoring, and managing risks. The program's RMIS will support management communication and facilitate planning and coordination, as appropriate.

Specific input data and output documents of the RMIS will be detailed in the RMIS system documentation. Figure 9 depicts the data flow concept for the risk management system.

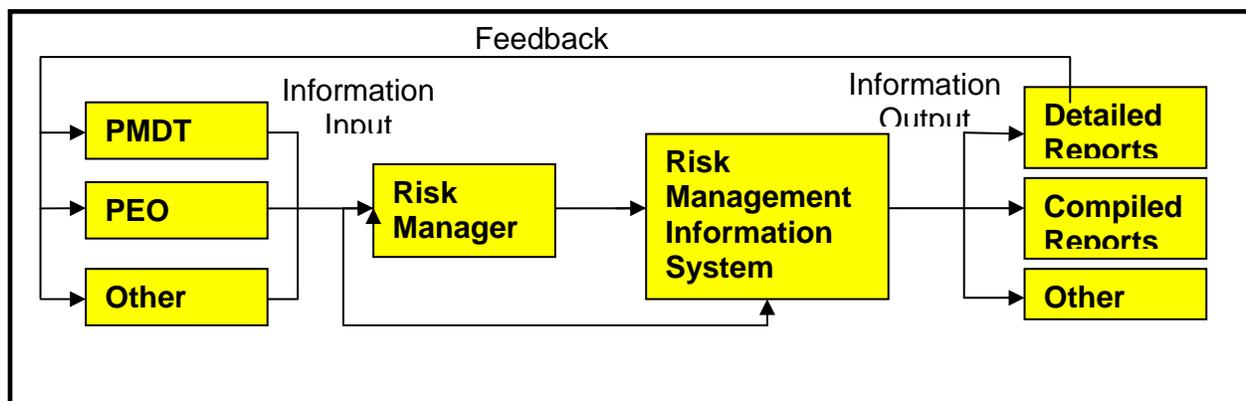


Figure 9: Risk Management Information Flow

Input for the RMIS originates from the Risk Assessment Form, as provided by the PMDT, PEO, and other stakeholders. The RMIS includes a database to manage existing and new risks. The database will support the following:

- Facilitation and coordination between metrics and risk control efforts
- Quick and convenient ways to develop supporting information for addressing program issues

- Determination of the effectiveness of risk indicators to support decisions
- Means to trace risk indicators to requirements
- Ability to evaluate risk indicator collection procedures
- Ability to collectively assess risks.

The RMIS will be capable of producing tailored reports for specific users. It can create outputs which are useful for other program objectives as listed below.

- Risk Matrix – A summary listing of risks with description, reported by, brief status, etc. See Figure 7.
- Risk Report – A summary document that tracks the status of the top risks. This report is provided to the PMDT on a monthly basis. Input is from the Risk Assessment Form.
- Risk Assessment Form - Serves as the RMIS input report, which contains all information necessary to satisfy the implementation of risk tracking and mitigation. Information includes mitigation and contingency plans related to the NECC risks.
- Detailed Risk Report - Provides the PMDT with information to make a decision on recommended control measure options. Includes details of risk control plans contained in Risk Assessment Forms. Describes the examination process for risk control options and gives the basis for selection of the recommended choice. Documents rationale for the PMDT's decision. Includes time-phased plan for the risk control task.
- Database Listing - The repository component of the RMIS. Contains all elements of risk.

### **5.10 Risk Management Training**

Getting the program team organized and trained to follow a disciplined, repeatable process for conducting a risk assessment (identification and analysis) is critical, since periodic assessments are needed to support major program decisions during the program life cycle. Experienced teams do not necessarily have to be extensively trained each time an assessment is performed, but a quick review of lessons learned from earlier assessments combined with abbreviated versions of these suggested steps could avoid false starts.

The program's risk coordinator may train the working groups, focusing on the program's RMP, risk strategy, definitions, suggested techniques, documentation, and reporting requirements. Training will be conducted on an as-needed basis or when requested by Working Groups or Branches.

## **APPENDIX A: GLOSSARY**

**Analysis** – The process of examining each identified risk area or process to define the description of the risk, isolating the cause, and determining the effects.

**Assessment** – The process of identifying and analyzing program area and critical technical processes risks to increase the probability/likelihood of meeting cost, schedule, and performance objectives.

**Control** – The process that identifies, evaluates, selects, and implements mitigation options so that risks can be managed and controlled within specified levels.

**Control Measure** – An implementation option that mitigates risks, or prevents the occurrence of potential risks.

**Cost Risk** – The risk associated with achieving life cycle cost goals. The foundation of cost risks is based on the risk of accurate cost estimates and the risk of not meeting cost goals due to program execution failures attributed to costs, schedule and performance problems.

**Identification** – The process of identifying program risks through interviews, surveys, and document searches.

**Mitigation** – The steps taken to either lessen the probability that a risk will occur or lessen the impact of the event upon the program

**Monitoring** – The process that systematically tracks and evaluates the behavior of risk control measures against pre-determined references throughout the acquisition process.

**Performance Risk** – The risk associated with the design and production of NECC technical capabilities that affect system performance levels and operational requirements.

**Risk** – A measure of the potential inability to achieve overall program objectives within defined cost, schedule, and performance constraints. The two components of risk are probability/likelihood of failing to achieve a potential outcome and the consequence/impact of failing to achieve that outcome.

**Risk Event** – An event within the program that could go wrong, that could result in negative impact on the program in any of the acquisition phases. A risk event can be characterized in

terms of likelihood of occurrence and its impact (or consequence) on the program. Example risk events include: (1) failure to adequately train system administrators, (2) failure to develop a software version transition plan within three months, and (3) failure to provide acquisition documents to the oversight organization by the suspense date.

**Risk Management Information System** - The RMIS is a software application that stores and sorts risks and generates risk management reports. The purpose of the RMIS is to provide a tool for tracking, monitoring, and managing risks. The program's RMIS will support management communication and facilitate planning and coordination as appropriate.

**Risk Reporting Matrix** – A graphical display of the level of risks identified within a program, determined by an assessment of the risks probability and impact. The level of risk for each root cause is reported as low (green), moderate (yellow), or high (red).

**Risk Rating** – A rating given to risks based on the probability of occurrence of the risk event and the impact of the risk event on the program.

**High Risk** – Unacceptable, major disruption likely. Different approach required. Priority management attention required.

**Moderate Risk** – Some disruption. Different approach may be required. Additional management attention may be needed.

**Low Risk** – Minimum impact. Minimum oversight needed to ensure risk remains low.

**Schedule Risk** – The risk associated with meeting estimated and allocated schedule milestones.

## APPENDIX B: ACRONYMS

Acronym	Definition
ABC	Adopt-before-Buy, Buy-before-Create
ACAT	Acquisition Category
ADM	Acquisition Decision Memorandum
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
C2	Command and Control
C2C	Command and Control Capability
CAIV	Cost as an Independent Variable
CARD	Cost Analysis Requirements Description
CDP	Capability Definition Package
CM	Capability Module
COI	Community of Interest
COTS	Commercial-Off-the Shelf
CPAS	Capability Provisioning Activities
CPMO	Component Program Management Office
DAA	Designated Accrediting Authority
DECC	Defense Enterprise Computing Center
DISA	Defense Information Systems Agency
DOD	Department of Defense
DOD CIO	Department of Defense Chief Information Officer
DOT_LPF-P	Doctrine, Organizational, Training, Leadership and Education, Personnel, Facilities, and Policy
DOL	Defense Online
ESOH	Environmental, Safety and Occupational Health
FDCE	Federated Development and Certification Environment
FoS	Family of Systems
GCCS	Global Command and Control System
GES	GIG Enterprise Services
GIG	Global Information Grid
GOTS	Government-Off-the-Shelf
IA	Information Assurance
IPT	Integrated Product Team
JCCD	Joint Combat Capability Developer
JPEO	Joint Program Executive Office

<b>Acronym</b>	<b>Definition</b>
JPM	Joint Program Manager
JPMO	Joint Program Management Office
JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Memorandum
KPP	Key Performance Parameter
LSA	Logistics Support Analysis
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MOA	Memorandum of Agreement
MS or M/S	Milestone
NCES	Net-Centric Enterprise Services
OTA	Operational Test Agency
OUSD	Office of the Under Secretary of Defense
PEO	Program Executive Office
PMDT	Program Management Direction Team
PM	Program Management
PPBE	Planning, Programming, Budgeting, and Execution System
RMP	Risk Management Plan
RMC	Risk Management Coordinator
RMIS	Risk Management Information System
SDD	System Development and Demonstration
SLA	Service Level Agreement
SOA	Service Oriented Architecture
TD	Technology Development
TDS	Technology Development Strategy
TOR	Terms of Reference
TRA	Technology Readiness Assessment
USJFCOM	United States Joint Forces Command
USMC	United States Marine Corps
USSTRATCOM	United States Strategic Command
WBS	Work Breakdown Structure
WIPT	Working-Level Integrated Product Team

## APPENDIX C: REFERENCES

- a. Interim Defense Acquisition Guidebook, October 30, 2003.
- b. Risk Management Guide for DoD Acquisition, Sixth Edition, August 2006.
- c. Guidelines for Successful Acquisition and Management of Software Intensive Systems: Weapon Systems, Command and Control System, and Management Information Systems," Version 3.0, Department of the Air Force, Software Technology Support Center, May 2000.
- d. Exhibit 300 Business Case Guide, Version 1.0, FY 2006 Budget Submission, Internal Revenue Service Capital Planning and Investment, March 5, 2004.
- e. DoD 5000.4, OSD Cost Analysis Improvement Group, 24 November 1992.
- f. DoD 5000.4-M, Cost Analysis Guidance and Procedures, December 1992.
- g. Program Managers Tool Kit, Defense Acquisition University, Thirteen Edition (Ver 2.0), February 2004.
- h. A Guide to the Project Management Body of Knowledge, PMBOK Guide 2000 Edition, Project Management Institute,
- i. DoD Extension to: A Guide to the Project Management Body of Knowledge, (PMBOK Guide) First Edition (Version 1.0) June 2003.
- j. Capability Maturity Model Integration (CMMI) SE/SW/IPPD/SS, Version 1.1.
- k. Capability Maturity Model Integration (CMMI) Acquisition Module (CMMI-AM), Version 1.0, February 2004.
- l. The Capstone Requirements Document, Global Information Grid (GIG), JROCM 134-01, 30 August 2001.
- m. OMB Circular A-76, Performance of Commercial Activities (Revised 29 May 2003).
- n. OMB Circular A-11, Part 7, Planning, Acquisition, and Management of Capital Assets, July 16, 2004.

## APPENDIX D: INCREMENT 1 RISKS

*This section is a summary of section 2.0 of the Cost Analysis Requirements Document (CARD) and identifies the program manager's assessment of the program and the measures being taken or planned to reduce those risks. Appendix D also lists the TD Phase risks that were initiated in June 2006 as part of the JPMO's initial risk assessment. Mitigation actions are ongoing throughout the TD Phase.*

### **Increment 1 Risks**

This appendix identifies the program manager's key risks and the measures being taken or planned to reduce those risks. It includes the TD phase risks that were initiated in June 2006 as part of the JPMO's initial risk assessment. Mitigation actions are ongoing throughout both the TD phase and the SDD phase. The NECC program is susceptible to programmatic, developmental, technological, security, supportability, and certification and accreditation risks.

#### ***Programmatic Risk***

NECC has a variety of programmatic risks including organizational risks, risks that come from being a Joint program, partnership risks, and other risks. These are summarized below.

Governance Risk NECC requires a structure to control programmatic actions in accordance with the Terms of Reference (TOR), which define roles and responsibilities for program participants. If this governance structure is not mature and functioning, NECC is at risk of completing necessary actions to transition from TD to SDD. The PMDT mitigates this risk through open review and implementation of the TOR and provides an open governance forum. (Tracked as TD Phase Risk 1, assessed as medium risk, with potential impacts to cost, schedule, and performance.)

Acquisition Streamlining A component of NECC is rapid delivery of CMs, and a comparable acquisition component is speedy delivery of acquisition documents and an efficient acquisition approach. The risk is that without streamlining the program takes longer to produce information, increasing costs. The program mitigates this risk through streamlined documentation, taking advantage of flexibility in the DOD 5000 series, and early involvement of stakeholders through the PMDT and WIPTs. (Tracked as TD Phase Risk 2, assessed as medium risk, with potential impacts to cost and schedule.)

Organizational Risk Organizational risk exists from the need of a Joint Major Defense Acquisition Program (MDAP) to be coordinated through the services and agencies throughout the OD. This risk manifests itself in the time required to staff documents and actions throughout the Department, which can delay major activities such as Milestone Decision Reviews. The risk also includes the potential of stakeholders to bring forward issues to the program which may not have been previously considered. To mitigate this risk, NECC uses the PMDT. The PMDT provides all stakeholders representation and participation in forward-looking cost, schedule, and system performance reviews. The PMDT provides organizational risk management by functioning as an integrated, organization-wide body that proactively identifies, assesses, and addresses risk in a quantifiable manner across all stakeholder operations.

Joint Risk JFCOM serves as the NECC requirements authority, working with the Warfighter to identify C2 needs, capabilities and gaps that are filled by NECC via C2 net-centric solutions.

Joint risk mitigation requires the Services and Agencies to seek a cohesive approach to C2 solutions in search of a “best of breed” capability. The risk is to ensure that the Service C2 requirements are properly mapped to NECC and those that cannot transfer are clearly identified so that the Services may budget for sustainment. To mitigate this risk, JFCOM created a JCCD organization where requirements are fully vetted in an open forum with all stakeholders, in order to ensure joint vice service-centric solutions. Additionally, the NECC PMDT actively engages its CPMO representatives from the Services and Agencies to relay Warfighter needs to the developers.

JCCD Process Risk The materiel development component of the JCCD process risk is equivalent to requirements risk (covered under Development Risks below). There is a TD phase exit criteria associated with the JCCD process. If it is not sufficiently demonstrated during the TD phase then the program cannot satisfactorily address the Acquisition Decision Memorandum (ADM) requirement. To mitigate this risk USJFCOM and the JPMO collaborate to produce CDPs and assess their utility during CPAS activities. (Tracked as TD Phase Risk 8, assessed as medium risk, with potential impacts to schedule and performance.)

Partnership Risk The NECC PM manages partnerships through Memoranda of Agreement (MOAs) which define the authority, roles and responsibilities of each partner. NECC Tier 1 Development Partners are under direct funding of the NECC JPEO and technical direction of the Chief Engineer and Technical Director. NECC Tier 2 Development Partners are not directly funded by NECC but produce software that is incorporated into the NECC baseline capability and implemented by CPMOs. NECC Tier 3 Developmental Partners are 3rd party efforts, programs, or systems that produce and deploy a capability, product, or data that is consumed by NECC and against which NECC requirements can be allocated. These partnerships will be characterized primarily by an MOA and Service Level Agreement (SLA) which establishes the necessary functional, technical and procedural relationships. The risk associated with these partnerships is that the partner does not produce the agreed product. The mechanism to mitigate this risk is similar to dependency risks below and includes the PMDT, Systems Engineering, and the Cost Control system. Each of these provides for proactive analysis and planning for alternatives in advance of issues impacting the program. (Tracked as TD Phase Risk 9, assessed as medium risk, with potential impacts to cost, schedule, and performance.)

Funding Risk Funding for any program is a potential risk, as programs are typically under-funded. The NECC program is not currently funded to achieve the objective CDD requirements. To mitigate funding risk, the JPMO leads forward planning activities to produce various courses of action. This allows the JPEO to anticipate required funding levels and coordinate with DISA and Office of the Under Secretary of Defense (OUSD) on funding needs and alternative solutions. Also, the JPEO works within the Planning, Programming, Budgeting, and Execution System (PPBE) process and through legislative liaison with the Congress in order to justify NECC funding levels and keep the Congress informed on program progress.

Cost Risk Cost risks are fully vetted in the Cost Analysis Requirements Description (CARD). To summarize, costs risks are managed through consistent and in-depth systems engineering, proactive use of contracting best practices, and use of cost and performance management systems (NECC uses a modified earned-value system). Mitigation includes use of appropriate program management reserve and Cost as an Independent Variable (CAIV) as required when the cost-control system indicates these actions are necessary.

### ***Development Risk***

Development risk considers uncertainty of the individual mission application to achieve or satisfy functional and technical requirements. Development risk also entails integration risk, which is the uncertainty of system integrators to produce an operable capability.

Requirements risk is a developmental risk where requirements may be developed late or stated incorrectly. This is not unusual, as software projects typically suffer from the simple fact that system requirements are not well understood at the start of a project. To mitigate this risk, NECC employs multiple activities. A key component is that NECC anticipates that not all requirements are fully clarified at program initiation, and the systems engineering process is specifically designed to accommodate emerging requirements. Another key program concept is basing NECC on transforming the Global Command and Control Systems Family of Systems (GCCS FoS), which gives a realistic operational predecessor system to allow the requirements managers and engineers to better understand and articulate the actual Warfighter need. The JCCD and systems engineering processes (to include ABC) are iterative, meaning there are reviews and feedback loops to ensure increased precision and understanding of requirements as they are developed and vetted. The implementation process is a spiral activity with full feedback via the FDCE, where all stakeholders can review and comment on the maturity of CMs throughout their development. The predecessor system together with multiple feedback loops and close interaction between users and developers ensure mitigation of requirements risk.

An aspect of developmental risk associated with requirements risk is that the program may have engineering estimates too low, or more development may be required than planned, resulting in increases in SLOC counts for the CMs. To mitigate these risks, the program's estimating models include additional work, and NECC uses CAIV as appropriate.

Developmental risks include integration and interoperability risks, where more work than planned may be required. To mitigate this risk, individual CMs use standardized data models and well established technical standards via the SOA to simplify integration and interoperability. A key function of the SOA is to assist integration by reducing the number of direct CM to CM interfaces, building in interoperability. A design element in the engineering process is for individual CMs to have few direct dependencies on each other. CAIV is also a mitigation practice to be used if integration or interoperability becomes cumbersome.

### ***Technology Risk***

Technology risk addresses uncertainty associated with the dependence of NECC on external technologies required for its implementation. The NECC Technology Development Strategy (TDS) identified nine technology shortfall areas:

- Cross-Domain/Cross-Coalition/Multi-Level Security Technologies
- Operator-Friendly Service Composition Tools
- Semantic Data Modeling Tools
- Data Management
- Enterprise-Level Quality of Service Management Tools and Services
- Performance Limitations of Current Services Technologies

- Testing and Certification of Service-Oriented Architectures
- 3-D Rendering Environments
- Software Distribution/Commercial-off-the-Shelf (COTS) Product Management

Technology risk reduction activities during the TD phase explore various mitigation processes for these risks. These nine technology shortfall areas form the basis for identification of the critical technology elements assessed as part of the Technology Readiness Assessment (TRA). The need to identify and assess new capabilities for NECC is a key component of ABC, and there is a risk that the current process is insufficient to properly take advantage of technology developments. The Program is working with a capability broker to mitigate this risk. (Tracked as TD Phase Risk 18, assessed as high risk, with potential impacts to performance.)

DIL Coalition Interoperability There is a TD phase exit criteria associated with the degraded, intermittent, or limited connectivity and coalition interoperability. If this capability is not sufficiently demonstrated during the TD phase then the program cannot satisfactorily address the ADM requirement. To mitigate this risk the systems engineering team plans and collaborates to demonstrate capability during CPAS activities. (Tracked as TD Phase Risk 10, assessed as medium risk, with potential impacts to cost, schedule and performance.)

Dependency Risk As with any business or activity, NECC depends on internal and external resources to achieve its objectives. Internal resources are managed via the JPEO, JPMO and CPMOs. The difficulty with external dependencies is that those resources are outside the control of the NECC PMs. Their availability, quality, and responsiveness can have adverse impact on NECC's development schedule. NECC uses a systems engineering approach tied to the JCCD requirements process to provide proactive analysis and understanding of dependencies in order to create robust strategies to mitigate these risks.

NECC is dependent on GCCS FoS, NCES, and GIG Transport. NECC evolves GCCS FoS applications from the current joint and Service variants into a single capabilities-based net-centric architecture. The dependency risk occurs when some components of the FoS can not be transitioned to NECC. To mitigate this risk, NECC engineers use a capability brokering concept and the ABC construct to ensure alternative solutions are fully reviewed and vetted before completely developing new capability.

NECC applications and functions are supported by the GIG Enterprise Services (GES), key NCES capabilities (discovery, security, messaging, and mediation), GIG Transport, and PKI technologies. NCES provides a common set of interoperable information capabilities to access, collect, process, store, disseminate, and manage information on demand for Warfighters, policy makers, and support organizations.

NECC uses the capability broker to ensure alternative solutions are available, and uses the Adopt-Before-Buy, Buy-Before-Create (ABC) acquisition approach to mitigate some of the technology risk that it faces. By looking to adopt existing capabilities first, NECC incurs a significantly smaller cost in comparison to buying a capability in the commercial community. If purchasing a capability that meets the requirements from the CDD is not feasible, then as a last

resort, NECC will look to create the capability. (Tracked as TD Phase Risk 7, assessed as medium risk, with potential impacts to cost, schedule, and performance.)

Authenticated Data Sources NECC has a dependency on authenticated data sources. If these are not available for piloting, then it will adversely impact the establishment of capacity-based piloting infrastructure and the program will be unable to address the associated ADM exist criteria #2. The program is mitigating this risk with planning and collaborating with external programs to support the piloting activities. (Tracked as TD Phase Risk 20, assessed as medium risk, with potential impacts to cost, and schedule.)

Knowledge Management Knowledge Management (described as Data Management in the TDS) risk is that pertinent information will not be readily available to users or stakeholders when they require it. NECC faces this risk with its reliance on the Defense Online (DOL) portal for distribution and accessibility of work products of its various branches within the program. The organization, consistency, and availability of programmatic information are essential to proper staffing and coordination of program data. To mitigate this risk NECC has standard policies and procedures for storing data on the DOL that all WGs follow in order to ensure consistency and ease of data retrieval.

### ***Security Risk***

Security Risk considers uncertainty associated with security vulnerabilities. NECC is a SECRET and TOP SECRET level command and control system requiring positive identification and authentication of users. It is operated by a combination of military personnel, government civilian and contractor personnel. All personnel that operate NECC are required to have a minimum of a SECRET security clearance. There is no public access to the system. Potential security vulnerabilities are identified and corrected/mitigated as an on-going process.

Security risks associated with CM development is that the Designated Accrediting Authority (DAA) may require accreditation of each CM, instead of globally accrediting NECC as a system. Early coordination with the DAA is used to mitigate this risk. Similarly, multiple certifications could be required at individual sites between separate security enclaves. The program mitigates this risk by working with the PAA to ensure the security approach is acceptable.

Since NECC relies on the FDCE, there is a risk that the Information Assurance (IA) community does not accept FDCE process as sufficient to ensure IA. To mitigate this risk the program is adding validation processes to the FDCE to ensure it complies with IA requirements.

### ***Supportability Risk***

Supportability risk addresses uncertainty of having sufficient support resources available such as appropriate personnel with the required skills and training; facilities for development, testing, and integration; documentation to support users; infrastructure to support the mission applications; and a software maintenance plan for the program. Supportability risks and mitigation practices follow.

The risk that Service/Component computing environments do not meet NECC requirements is mitigated by pre-planning and test activities. If it turns out that CPMO-hosting of Local Nodes requires more servers than estimated, the program must procure additional server hardware. In this fashion, if more than five Defense Enterprise Computing Centers (DECCs) are required by NECC to support the software at the enterprise level, the program will mitigate this risk by

contracting for additional services (DECCs are fee-for-service). (Tracked as TD Phase Risk 16, assessed as medium to low risk, with potential impacts to cost and performance.)

In the case where NECC does not provide the required quality of service, additional nodes and hardware can be added to improve the overall quality of service. This risk is considered low given that the DECCs are structured to provide load balancing and redundancy for the program.

A risk exists that licenses for all common SW components can not be procured through the Joint program. The program mitigates this risk by using DISA/DOD to assist with licensing, or by having the CPMOs negotiate individually if required.

NECC may be at risk when using network-based distribution for fielding and installation of software. To mitigate this risk, the program is continuing to research and develop network approaches for software distribution. If this is unsuccessful, onsite delivery and installation will be used.

Training Training is a Key Performance Parameter (KPP). The risk exists that it may be unacceptable for the Training KPP not to be fully met until Increment 3. To mitigate this risk, the program intends to use Government-off-the-Shelf (GOTS)/COTS training materials for adopted or purchased CMs. For new CMs, the program uses industry cost models for development of training materials and allocates additional costs for training system development. (Tracked as TD Phase Risk 19, assessed as medium risk, with potential impacts to cost and schedule.)

Manpower The program may have understated the risk of operational manpower. To mitigate this risk the program intends to use net-centric capabilities to reduce manpower in the field and to use learning curve theory which should provide for fewer users over time.

The Help Desk support may prove to be insufficient. The program is currently planning for high utilization of the Help Desk at early implementation and can allocate additional manpower to provide support and mitigate the overall risks.

### ***Test Certification/Accreditation Risk***

Test risk is the possibility of not adequately testing NECC capabilities prior to their release to the Warfighter for operational use. Robust testing minimizes “surprises” when the product is sent to the Warfighter and ensures the specified capabilities are evaluated in the operational environment. Risk is reduced by bringing all testing agents together early in the process to ensure capabilities are tied to missions and tasks, mission-based testing is conducted, system anomalies/deficiencies are identified early in the process, and all data are shared.

The NECC test strategy is designed to reduce the risks involved with fielding. Since NECC is a Joint program, DISA, the Combatant Commands, and the Services will collaborate to establish the processes for CM development, integration and testing. To minimize risks, NECC will enable the use of piloting. Piloting will be used as a key mechanism during CM development and will provide a robust environment for CM testing. Piloting, in the context of NECC, is a concept for introducing capabilities to users, exposing them to other capabilities early in the CM development process, and ensuring they remain available to Warfighters and to other capabilities throughout the CM life cycle.

Test, Certification, and Accreditation risk involves uncertainty associated with a capability’s ability to satisfy testing, certification, and accreditation criteria. Key risks involve the potential

for the FDCE to be unavailable or not fully functional or to require more hardware or software to function correctly. To mitigate these risks the FDCE has been designed for expansion, and can incorporate additional hardware and software systems. If the FDCE does not suffice for NECC, traditional manual approaches to test, certification, and accreditation can be used. An FDCE risk exists in the TD Phase exit criteria for process maturity. If the FDCE is not shown as sufficiently mature then the program cannot satisfactorily address the ADM requirement. To mitigate this risk, the NECC team is planning for work-a-rounds and will determine the maturity of each process on the FDCE, as well as mitigating risks as described above. (Tracked as TD Phase Risk 11, assessed as medium risk, with potential impacts to cost, schedule, and performance.)

An FDCE availability risk was tracked in the TD Phase as Risk 12, assessed as high risk, with impacts to cost, schedule and performance. The team is mitigating this risk by identifying and employing manual work-a-rounds as the FDCE matures and becomes available for use.

There is also a risk that current manning for the evaluation processes may be insufficient. To mitigate this risk the teams are performing extensive planning to anticipate requirements, and may use additional manpower as required. (Tracked as TD Phase Risk 13, assessed as high risk, with potential impacts to cost, schedule, and performance.)

A small risk exists that an OTA is unavailable to support test. With five Operational Test Agencies (OTAs) involved in planning, there is no single dependency on an individual OTA that can not be shifted to another test agency. The risk that each OTA requires testing is being mitigated by planning for the “test once practice” where a single test serves for all OTAs. With all OTAs involved in all aspects of test process the program assesses this risk as low.

A comprehensive test, evaluation, and certification risk exists in the TD phase exit criteria for process maturity. If test, evaluation, and certification ability is not sufficiently demonstrated during the TD phase then the program cannot satisfactorily address the ADM requirement. To mitigate this risk the test and evaluation team is collaborating closely with the OTAs to demonstrate test, evaluation, and certification ability during TD phase CPAS activities. (Test and Evaluation tracked as TD Phase Risk 5, assessed as high risk, with potential impacts to cost, schedule, and performance. Certification and accreditation risk tracked as TD Phase Risk 6, assessed as high risk, with potential impacts to cost and schedule.)

## APPENDIX E: TD PHASE RISKS

	Area	Description	Risk Statement
1	Governance Structure	Overall joint governance and organizational structure, to include functions, roles & responsibilities, and processes	If a mature, functioning governance structure IAW the NECC Terms of Reference is not in place by the end of the TD phase, then timely decisions and follow-on actions required to prepare for the SDD phase cannot be completed, and SDD phase activities cannot be properly executed.
2	Acquisition Streamlining	Streamline overall acquisition approach including statutory and regulatory information requirements	If the overall acquisition approach cannot be streamlined, then the program will be unable to deliver planned increments as quickly as necessary to meet NECC program objectives.
3	Funding Strategy	Execution process/strategy for NECC funds; how funds will move.	If the execution process for NECC funds is not finalized/established, then the program will be unable to develop an Acquisition Strategy and Acquisition Program Baseline to satisfy Milestone B requirements.
4	Technology Issues	Technology required for Increment 1 SDD in a relevant environment via TD phase CM piloting to include coalition-interoperable nodes	If the technology issues relevant to Increment 1 SDD phase development are not resolved during the TD phase, then the program will be unable to satisfactorily address the associated ADM exit criteria, and therefore unable to reach Milestone B.
5	Test, Evaluation & Certification Process	A set of processes for the federated testing, evaluation, and accreditation of Capability Modules developed within the FDCE.	If the program is unable to demonstrate that the test, evaluation, and certification processes have sufficient maturity for successful SDD phase execution, then the program will be unable to satisfactorily address the associated ADM exit criteria, and therefore unable to reach Milestone B.
6	Information Assurance Certification & Accreditation Process	A set of processes for Information Assurance testing, certification, and accreditation of Capability Modules developed within the FDCE.	If the program is unable to demonstrate that the information assurance certification and accreditation processes have sufficient maturity for successful SDD phase execution, then the program will be unable to satisfactorily address the associated ADM exit criteria, and therefore unable to reach Mileston B.
7	External Dependencies (e.g., NCES, Data Strategy, GIG Standards)	Technology solutions and/or mandated standards expected to be provided by/available from non-NECC programs or non-programmatic organizations.	If the technology solutions and/or mandated standards expected to be provided by/available from non-NECC organizations are not available/mature, then the NECC program will have to either provide these products at the expense of program cost and schedule, or descope/rescope intended capabilities to be delivered in Increment 1.
8	JCCD Process	The process designed to determine, articulate, assess, prioritize and document NECC program capability needs	If the JCCD process is not sufficiently demonstrated during the TD phase, then the program will be unable to satisfactorily address the associated ADM requirement, and therefore unable to reach Milestone B.
9	Collaborative Development & Partnerships	Environment and processes necessary to ensure the ability to execute the NECC process for the SDD phase	If the collaborative development and partnership environment and related processes are not sufficiently mature in the TD phase, then the program will be unable to satisfactorily address the associated ADM requirement, and therefore unable to reach Milestone B.