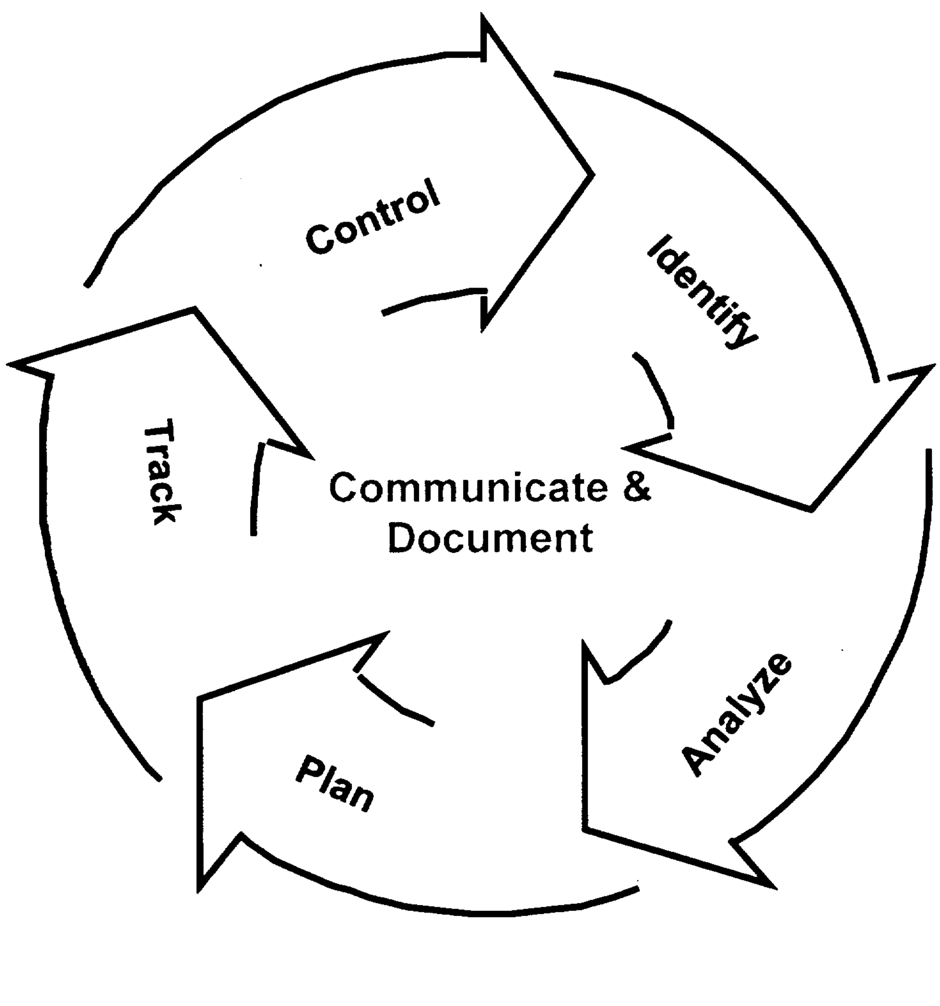
National Aeronautics and
Space Administration

Continuous Risk Management Course



This course is being taught by the Software Assurance Technology Center (SATC). For information contact Ted Hammer, Code 302, 301-286-7123.

Rev 2, 1/99

Table of Contents

Module 1

Welcome

Overview

Introductions

Facilities

Course Objectives

Course Schedule

Style of Course

Course Materials

Software Assurance Technology Center

Develop and apply assurance technology for software products

Primary task areas:

- Software Metrics
- Assurance Tools & Techniques
- Guidebooks & Standards
- Applied Research and Project Support

Web page:http://satc.gsfc.nasa.gov

Facilities

Restrooms

Emergency exits

Messages/phones

Lunch/breaks

Targeted Audience

Mix of project personnel and change agents with variable levels of experience development projects

Prerequisites:

- engineering experience (at least one year)

Assumptions:

- prior knowledge of risk or risk management unnecessary

Course Objectives

Understand the concepts and principles of Continuous Risk Management and how to apply them

Develop basic risk management skills for each component of Continuous Risk Management

Be able to use key methods and tools

Be able to tailor Continuous Risk Management to a project

Course Schedule

One Day

1. Welcome
2. Paradigm Overview
3. Identify
4. Analyze
5. Plan
6. Track
7. Control
8. Communicate & Document
9. Getting Started in Continuous Risk Management
10. Summary

Style of Course

Interactive

Lecture mixed with examples and discussion topics

Exercises

Case study - hypothetical but NASA-based

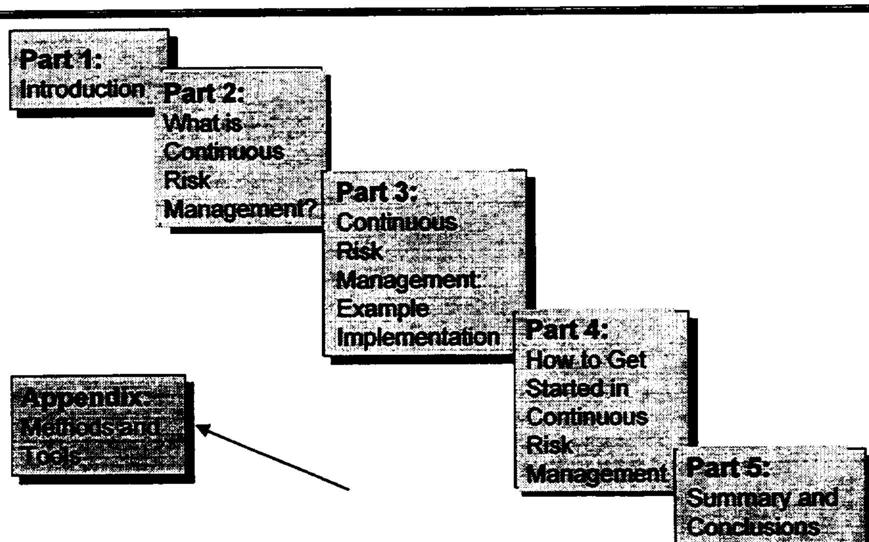
Course Materials

Student notebook

- **Case study**
- **List of Risks**

Continuous Risk Management Guidebook

Guidebook Organization



Module 2

Introduction

Overview

What is risk?

How is risk related to project management?

Why do risk management?

What is continuous risk management?

Drivers for continuous risk management?

Where is continuous risk management applied?

When should risk management be done?

Risk Management Plan

Who does continuous risk management?

Definitions of Risk

Risk is the potential for realization of unwanted negative consequences of an event.
- Rowe, *An Anatomy of Risk*

Risk is the measure of the probability and severity of adverse effects.
- Lowrance, *Of Acceptable Risk*

Risk is the possibility of suffering loss.
- Webster, *Third New International Dictionary*

Risk is the probability that a project will experience undersirable consequences.
- *NASA-NPG: 7120.5A*

Definitions of Risk

Risk always involves the <u>likelihood</u> that an undesired event will occur.

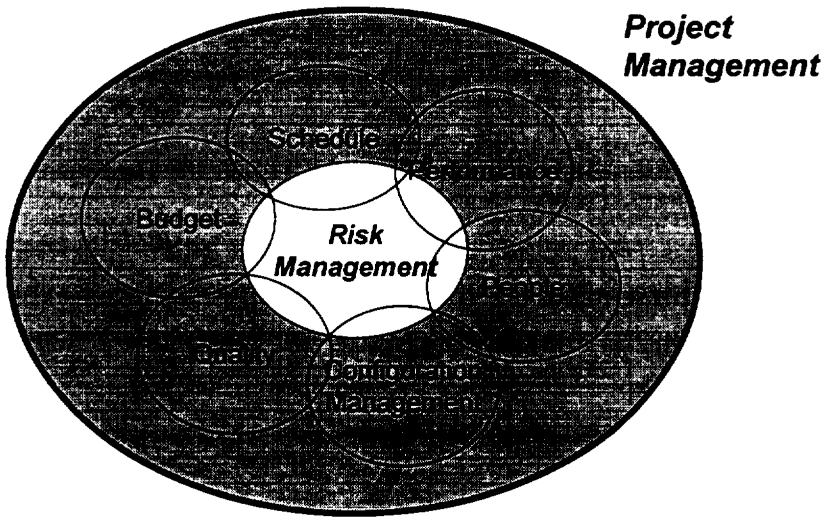
Risk should consider the <u>severity of consequence</u> of the event should it occur

Qualitative or Quantitative

Qualitative or Quantitative

Risk = Likelihood * Severity

Risk Management & Project Management



Why Do Risk Management?

- Early identification of potential problems
- Increase chances of project success
- Enable more efficient use of resources
- Promote teamwork by involving personnel at all levels of the project
- Information for tradeoffs based on priorities and quantified assessment

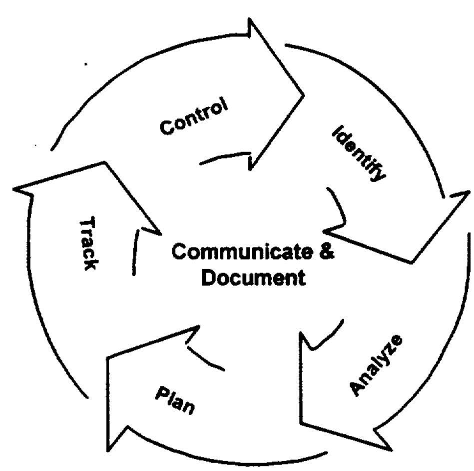
What is Continuous Risk Management?

A management practice with processes, methods, and tools for managing risks in a project.

It provides a disciplined environment for proactive decision making to:

- assess continually what could go wrong (risks)
- determine which risks are important to deal with
- implement strategies to deal with those risks
- assure, measure effectiveness of the implemented strategies

Continuous Risk Management



Components of Continuous Risk Management - 1

Identify

- search for and locate risks before they become problems

Analyze

- convert risk data into useable information for determining priorities and making decisions

Plan

- translate risk information into planning decisions and mitigating actions (both present and future), and implement those actions

Components of Continuous Risk Management - 2

Track

- monitor risk indicators and mitigation actions

Control

- correct for deviations from the risk mitigation plans and decide on future actions

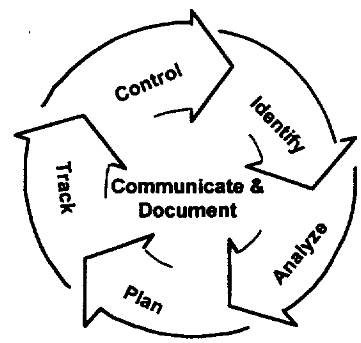
Communicate & Document

- provide information and feedback to the project on the risk activities, current risks, and emerging risks

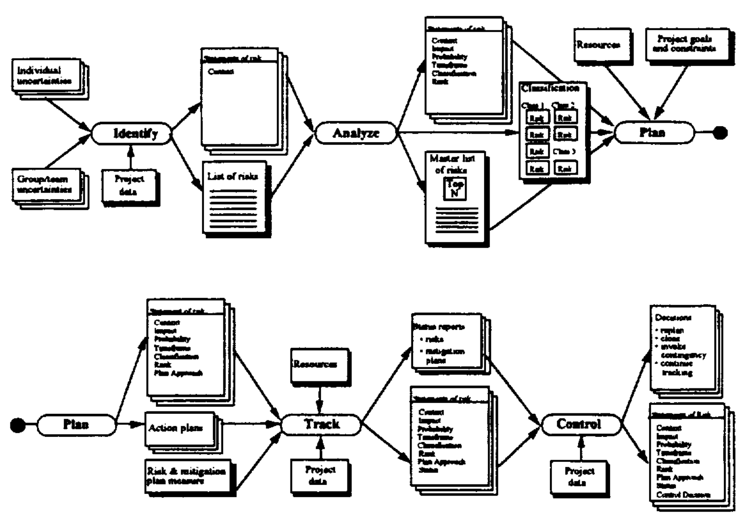
Relationship Among Functions

Throughout the project life cycle, risk components evolve

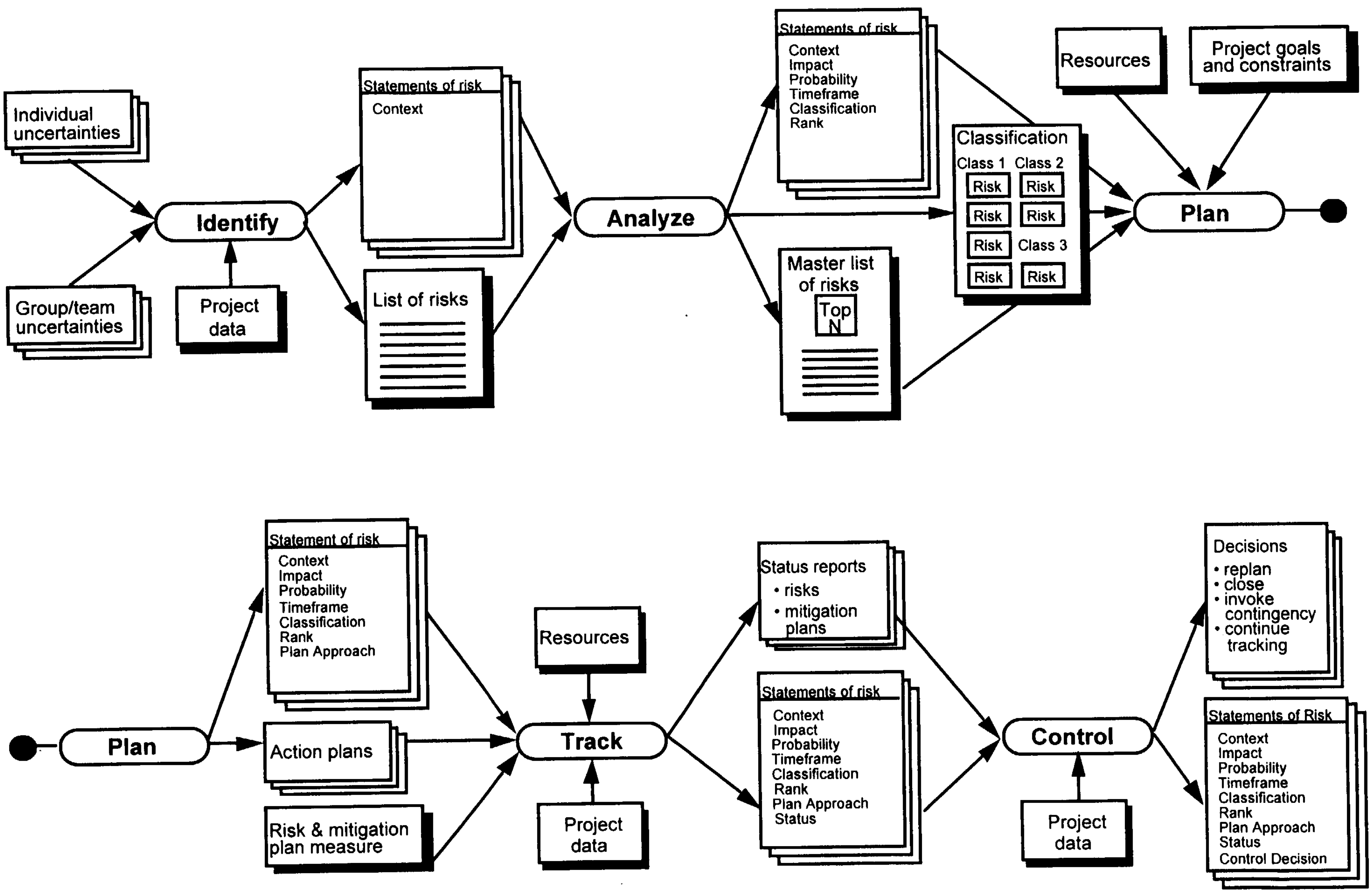
- continuously
- concurrently
- iteratively



Risk Management Data Flow



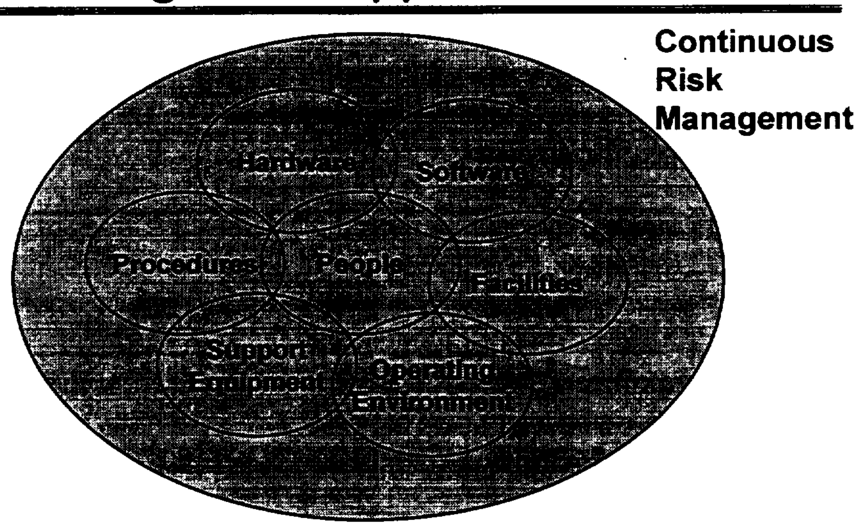
Risk Management Data Flow



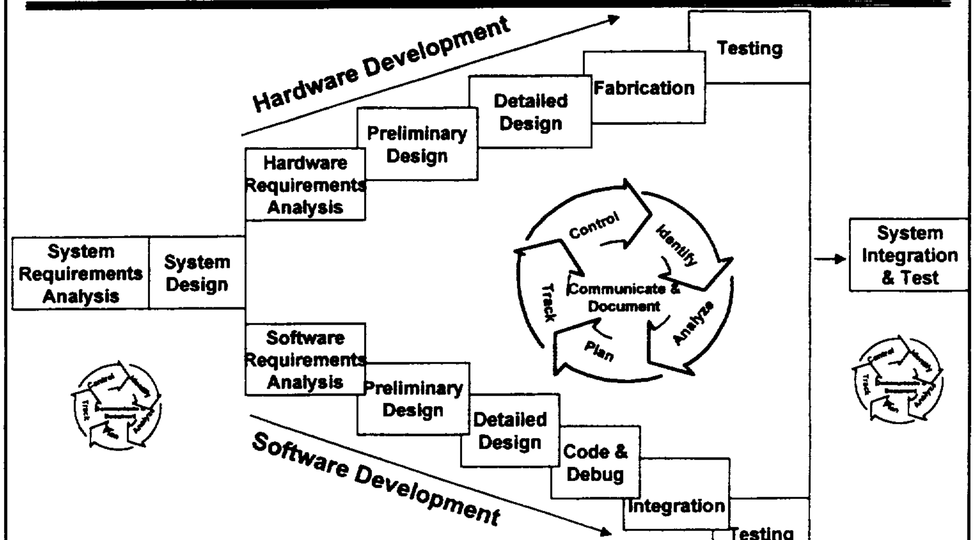
Drivers for Continuous Risk Management

- •NASA NPG 7120.5A: NASA Program and Project Management Process and Requirements
- •NASA-SP-6105: NASA Systems Engineering Handbook
- •ISO 9001: Quality systems
- •OMB Circular A-11: Planning, Budget & Acquisition
- •IEEE: P1448 - EIA PN3764 (ISO/IEC 12207): Standard for Information Technology
- •DoD: Military Standard Handbook 338: Electronic & Reliability Design Handbook
- •DoD: Military Standard 499: Engineering Management

Where is Continuous Risk Management Applied?



When Should Continuous Risk Management be Done?



Risk Management Plan

Definition

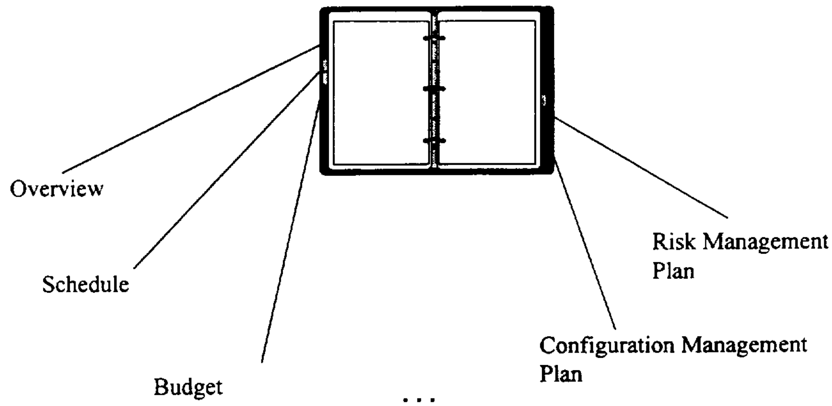
- documents the risk management practice (processes, methods, and tools) to be used for a specific project

Contents

- overview
- project organization, roles, responsibilities
- practice details (e.g., how are risks identified?)
- risk management milestones (e.g., quarterly rebaselining)
- risk information documentation (e.g., database)

Guidebook pp. 451-455

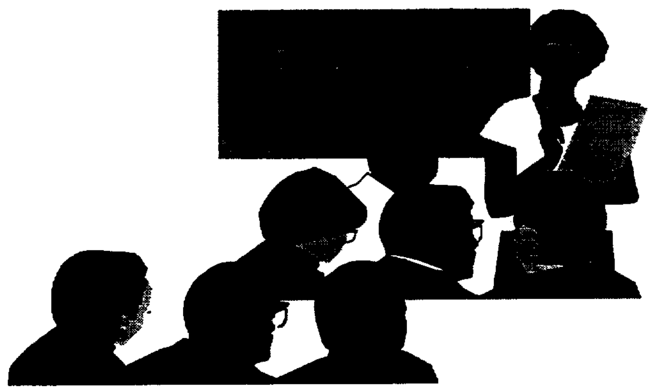
Project Management Plan



Relationship to Everyday Practice

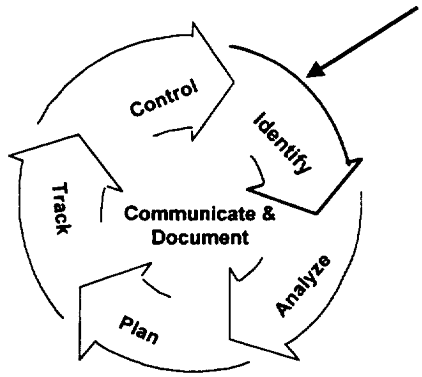
Learning
Continuous Risk Management
is similar to incorporating
any new habit
into your daily life.

Who Does Continuous Risk Management?



Module 3

Identify



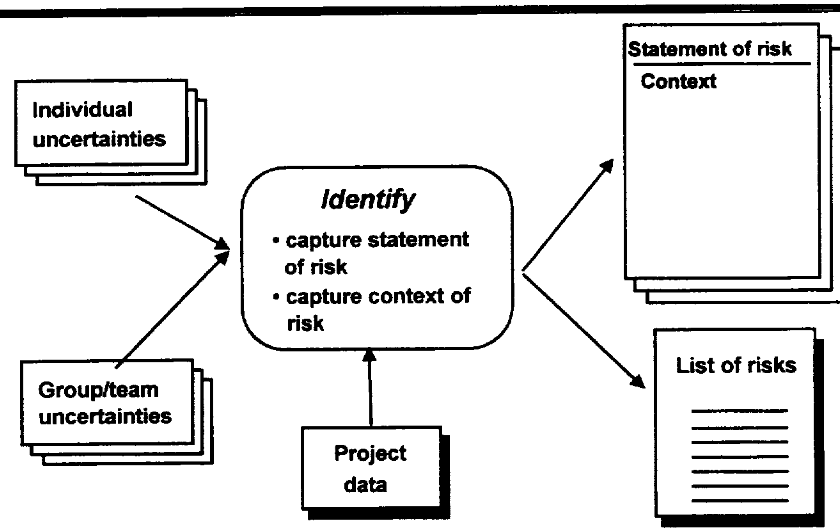
Overview

Activities overview

Identification activities
- **capturing statements of risk**
- **capturing the context of a risk**

Identification methods and tools
- **Examples**
- **Brainstorming**
- **Questionnaires and checklists**

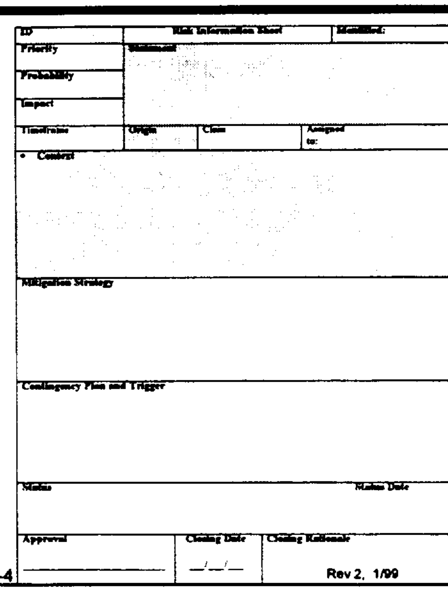
Identification Activities Overview



Recording Data on Risk Information Sheet

–Risk information sheet
–NASA Risk Management database

Complete:
- ID
- Date Identified
- Risk statement
- Origin
- Risk Context



Risk Information Sheet

ID	**Risk Information Sheet**			**Identified:** _
Priority	**Statement**			
Probability				
Impact				
Timeframe	**Origin**	**Class**	**Assigned to:** ____________	
• **Context**				
Mitigation Strategy				
Contingency Plan and Trigger				
Status			**Status Date**	
Approval ____________	**Closing Date** __/__/__	**Closing Rationale**		

Capturing Statements of Risk - 1

Purpose:

- **arrive at a concise description of risk, which can be understood and acted upon**

Description:

- **involves considering and recording the <u>condition</u> that is causing concern for a potential loss to the project, followed by a brief description of the potential <u>consequences</u> of this condition**

Components of a Risk Statement

Given the	**Condition**	;	*there is a possibility that* →	**Consequence**	*will occur*

Risk Statement

<u>Condition</u>: a single phrase briefly describing current key circumstances, situations, etc. that are causing concern, doubt, anxiety, or uncertainty

<u>Consequence</u>: a single phrase or sentence that describes the key, negative outcome(s) of the current conditions

Elements of a Good Risk Statement

Consider these questions when looking at a risk statement:

- Is it clear and concise?
- Will most project members understand it?
- Is there a clear condition or source of concern?
- If a consequence is provided, is it clear?
- Is there only ONE condition followed by one (or more) consequence?

Example Risk Statements

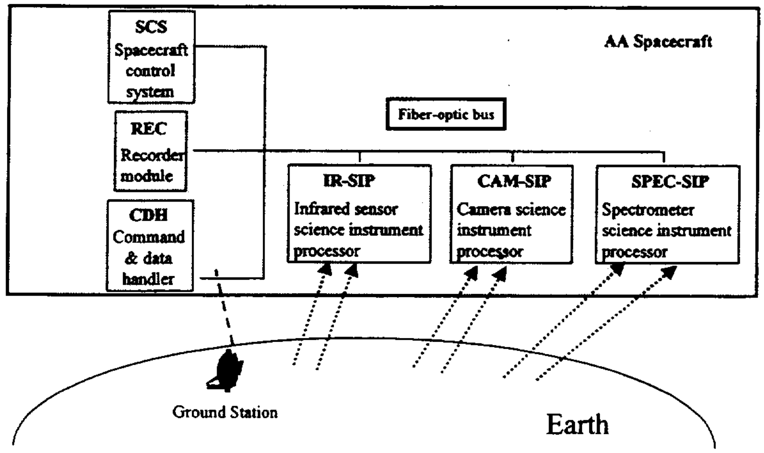
Good or bad risk statements?

1. Object Oriented Development !

2. The staff will need time and training to learn object oriented development.

3. This is the first time that the software staff will use OOD; the staff may have a lower-than-expected productivity rate and schedules may slip because of the associated learning curve.

Case Study Introduction



AA Spacecraft Hardware Architecture

IR-SIP Risk Statement Example #1

Commercial parts are being selected for space flight applications, and their suitability to meet environmental conditions is unknown; these parts may fail to operate on-orbit within the environment window, leading to system level failures. Also, environmental testing of these parts can be expensive and cause schedule delays.

Exercise -Writing a Risk Statement

IR-SIP Case Study - top pg 3 - under Engineering Considerations:

"2. A new high-speed fiber-optic data bus will be used so that high data transfer rates can be sustained."

Risk: Condition:

Consequence:

Possible Risk Statement

"2. A new high-speed fiber-optic data bus will be used so that high data transfer rates can be sustained."

Risk #2:
The high-speed fiber-optic data bus is untested technology; the bus may not perform as specified and high data transfer rates might not be sustained.

Capturing the Context of a Risk

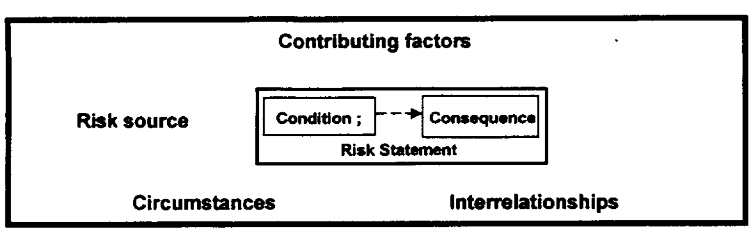
Purpose:

- provide enough additional information about the risk to ensure that the original intent of the risk can be understood by other personnel, particularly after time has passed

Description:

- capture additional information regarding the circumstances, events, and interrelationships not described in the statement of risk

Context



<u>Context</u>

An effective context captures the what, when, where, how, and why of the risk by describing the circumstances, contributing factors, and related issues (background and additional information that are NOT in the risk statement).

Elements of Good Context?

Consider these questions when looking at the context.

- Can you identify which risk statement this context is associated with?
- Is it clear what the source or cause of the risk is?
- Is it clear what the impact might be?
- Would you know who to assign the risk to for mitigation? Would they know what to do?
- Would you be able to tell if the risk has gone away?

Example Context - 1

Risk statement:
This is the first time that the software staff will use OOD; the staff may have a lower-than-expected productivity rate and schedules may slip because of the associated learning curve.

Good or bad context?

- It's a typical NASA project - new concepts without training.

Example Context - 2

<u>Risk statement:</u>

This is the first time that the software staff will use OOD; the staff may have a lower-than-expected productivity rate and schedules may slip because of the associated learning curve.

<u>Context:</u>

Object oriented development is a very different approach that requires special training. There will be a learning curve until the staff is up to speed. The time and resources must be built in for this or the schedule and budget will overrun.

Example Context - 3

<u>Risk statement</u>: Commercial parts are being selected for space flight applications and their suitability to meet environmental conditions is unknown; these parts may fail to operate on-orbit within the environment window, leading to system level failures. Also, environmental testing of these parts can be expensive and cause schedule delays.

<u>Context</u>:Although commercial parts are more readily available and have lower prices than space qualified parts, they have not been subjected to space environment conditions or levels. In particular, radiation effects can cause these parts to fail since they were manufactured without radiation in mind. Radiation testing can be expensive, and if the selected parts fail to meet requirements, procurement of space qualified replacement parts have long procurement lead times.

Exercise

Writing Risk Statements

Exercise: Writing Risk Statements

Based on the material you have just read, working with your group, write 2-3 risk statements. When you are done chose one risk and write it on the board.

Condition	;	Consequence

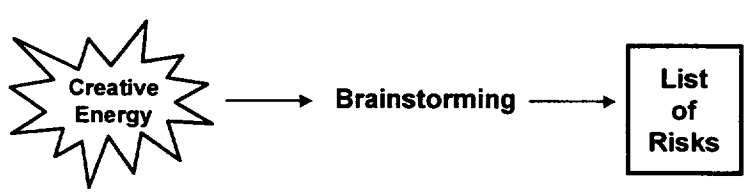
Risk Statement Sample Solutions

- This is the first time the IR Instrument Project manager is managing a project to go into space; Project may fail due to insufficient / poor management.
- There is a lack of a thorough hardware test program; mission failure due to environmental conditions not tested.
- Project software schedule and resources were underestimated; Schedule slips, cost overruns, and a reduction in adequate testing time are likely results.
- Science requirements have substantial TBDs; late completion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.

Brainstorming

Purpose:
- group method for generating ideas

Description:
- participants verbally identify ideas as they think of them, thus providing the opportunity for participants to build upon or spring off of ideas presented by others



Taxonomy-Based Questionnaire (TBQ)

definition:

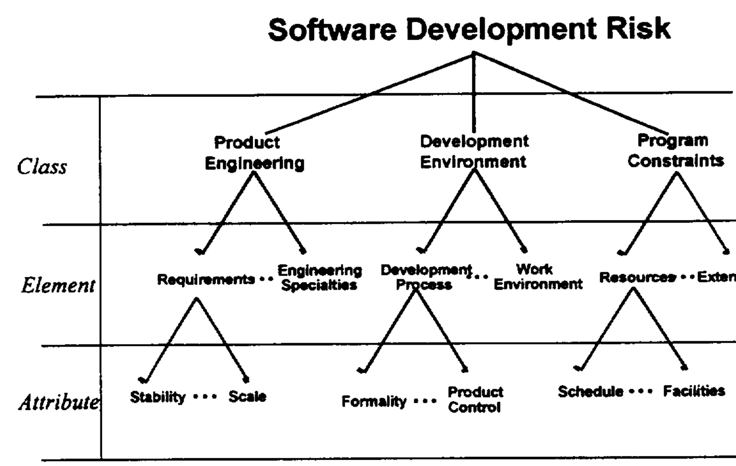
"... a scheme that partitions a body of knowledge and defines the relationships among the pieces. It is used for classifying and understanding the body of knowledge."

IEEE Software Engineering Standards **Collection, Spring 1991 Edition**

example:

A questionnaire organized according to the taxonomy of software development for the purpose of identifying risks by interviewing a group of one or more individuals.

Example -SEI Taxonomy Structure



Example TBQ Questions

Guidebook pp. 471- 493

Class	A. Product Engineering
Element	2. Design
Attribute	d. Performance *[Are there stringent response time or throughput requirements?]*
Starter	[22] Are there any problems with performance?
Cues	• throughput • scheduling asynchronous real-time events • real-time response • recovery timelines • response time • database response, contention, or access
Starter	[23] Has a performance analysis been done?
Follow-up	(Yes) [23.a] What is your confidence in the performance analysis? (Yes) [23.b] Do you have a model to track performance through design and implementations?

Goal/Question/Metric Paradigm GQM

Mechanism for formalizing the characterization, planning, construction, analysis, learning and feedback tasks

Three Steps:

1. **Generate a set of *goals* based upon the needs of the organization.**
2. **Derive a set of *questions*.**
3. **Develop a set of *metrics* which provide the information needed to answer the questions.**

(Solution to: How do we start?)

NASA Software Checklist

Organized by development phases of a project, with emphasis on the software portion of the overall project lifecycle.

Listed are *some*, not an exhaustive list, of the generic risks that should be considered when any project contains software. Entire list in Appendix of course notes.

Contains practical questions that were gathered by experienced NASA engineers.

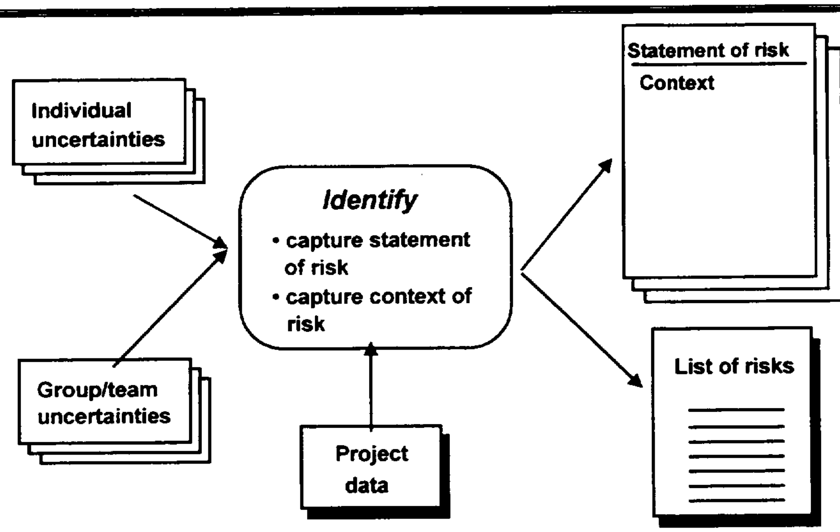
NASA Software Checklist - Partial

System Requirements Phase	RISK Yes/No /Partial	ACTION Accept/ Work
Are system-level requirements documented? To what level? Are they clear, unambiguous, verifiable ?		
Is there a project-wide method for dealing with future requirements changes?		
Have software requirements been clearly delineated/allocated?		
Have these system-level software requirements been reviewed, inspected with system engineers, hardware engineers, and the users to insure clarity and completeness?		
Have firmware and software been differentiated; who is in charge of what and is there good coordination if H/W is doing "F/W"?		
Are the effects on command latency and its ramifications on controllability known?		
Is an impact analysis conducted for all changes to baseline requirements?		

Mil Std 338 Design Checklist - Partial

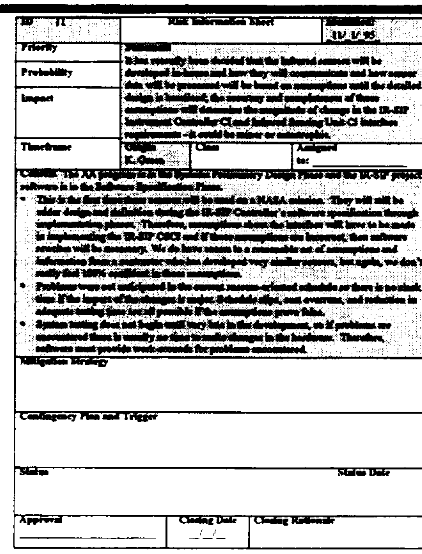
- Is the design simple? Minimum number of parts?
- Are there adequate indicators to verify critical functions?
- Are reliability requirements established for critical items?
- Are standard high-reliability parts being used?
- Have parts been selected to meet reliability requirements?
- Are circuit safety margins ample?
- Has provision been made for the use of electronic failure prediction techniques, including marginal testing?
- Have normal modes of failure and magnitude of each mode for each item or critical part been identified?
- Has redundancy been provided where needed to meet specified reliability?
- Does the design account for early failure, useful life and wear out?

Identification Summary



Risk Information Sheet

After Identify



ID 11	Risk Information Sheet	Identified: 11/1/95
Priority	Statement [illegible]	
Probability		
Impact		
Timeframe	Origin K. Green	Class / Assigned to:

Context: [illegible]

Mitigation Strategy

Contingency Plan and Trigger

Status | Status Date

Approval | Closing Date __/__/__ | Closing Rationale

Case Study

Risk Information Sheet After Analysis

<table>
<tr><td>ID 11</td><td colspan="3">Risk Information Sheet</td><td>Identified:
11/ 1/ 95</td></tr>
<tr><td>Priority 10</td><td colspan="4" rowspan="3">Statement
It has recently been decided that the Infrared sensors will be developed in-house and how they will communicate and how sensor data will be processed will be based on assumptions until the detailed design is baselined; the accuracy and completeness of those assumptions will determine the magnitude of change in the IR-SIP Instrument Controller CI and Infrared Sensing Unit CI interface requirements - it could be minor or catastrophic.</td></tr>
<tr><td>Probability M</td></tr>
<tr><td>Impact H</td></tr>
<tr><td>Timeframe N</td><td>Origin
K. Green</td><td>Class
Requirements</td><td colspan="2">Assigned
to: ____________</td></tr>
<tr><td colspan="5">Context The AA program is in the Systems Preliminary Design Phase and the IR-SIP project software is in the Software Specification Phase.
This is the first time these sensors will be used on a NASA mission. They will still be under design and definition during the IR-SIP Controller's software specification through implementation phases. Therefore, assumptions about the interface will have to be made in implementing the IR-SIP CSCI and if those assumptions are incorrect, then software rewrites will be necessary. We do have access to a reasonable set of assumptions and information from a contractor who has developed very similar sensors, but again, we don't really feel 100% confident in those assumptions.
Problems were not anticipated in the current success-oriented schedule so there is no slack time if the impact of the changes is major. Schedule slips, cost overruns, and reduction in adequate testing time are all possible if the assumptions prove false.
System testing does not begin until very late in the development, so if problems are encountered there is usually no time to make changes in the hardware. Therefore, software must provide work-arounds for problems encountered.</td></tr>
<tr><td colspan="5">Mitigation Strategy</td></tr>
<tr><td colspan="5">Contingency Plan and Trigger</td></tr>
<tr><td colspan="4">Status</td><td>Status Date</td></tr>
<tr><td colspan="2">Approval
____________</td><td>Closing Date
__/__/__</td><td colspan="2">Closing Rationale</td></tr>
</table>

Identification Key Points

$\boxed{\text{Condition;}} \rightarrow \boxed{\text{Consequence}}$
Risk Statement

A good risk statement
- contains ONLY one condition
- contains at least one consequence
- is clear and concise

Good context
- provides further information not in the risk statement
- ensures that the original intent of the risk can be understood by other personnel, even after time has passed
- Communication is an integral part of risk identification.

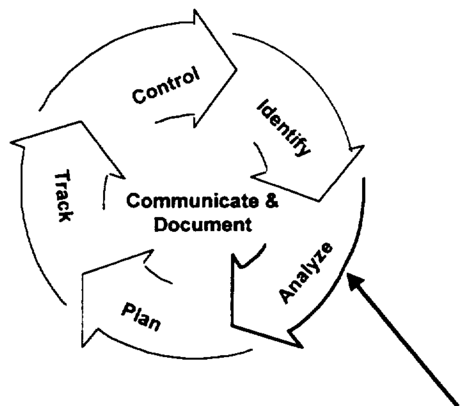
Identification Methods and Tools

- Risk information sheet
- Brainstorming
- Periodic risk reporting
- Voluntary Risk Reporting
- Taxonomy-based questionnaire (TBQ)
- Project metrics and Goal/Question/Metric*
- NASA software risk checklist*
- Mil-Std 338: Electronic & Reliability Design Handbook (HW)*

* Not in Guidebook

Module 4

Analyze

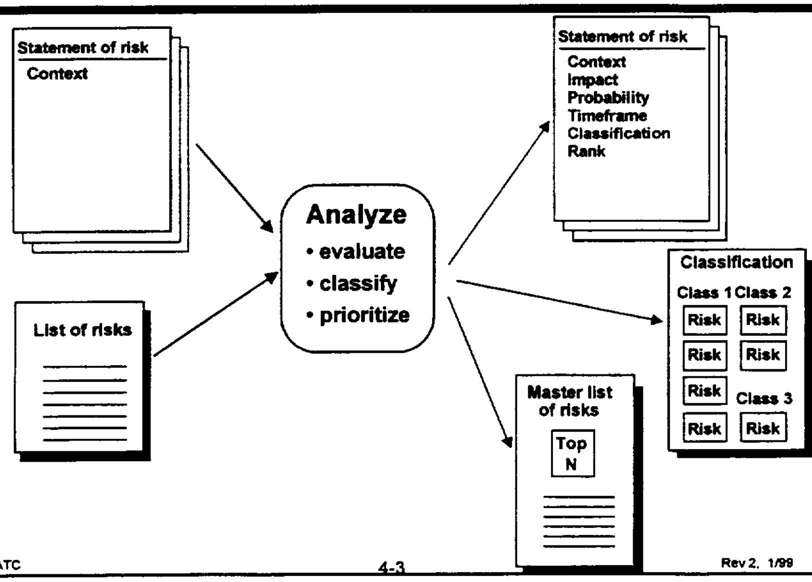


Overview

Analysis activities overview

Analysis activities
- **evaluating attributes of risk**
- **classifying risks**
- **prioritizing risks**

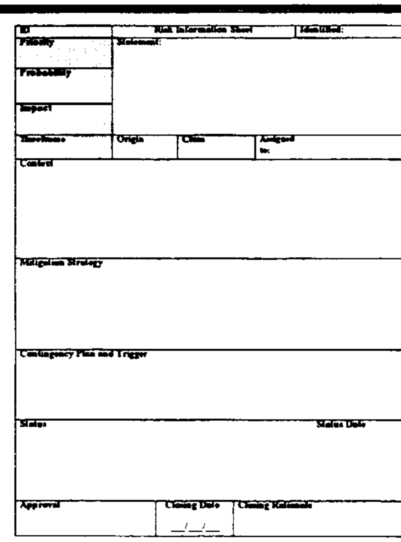
Analysis Activities Overview



Analysis - Risk Information Sheet

Related areas:

- Priority
- Probability
- Impact
- Timeframe
- Class



ID	Risk Information Sheet		Identified:
Priority	Statement:		
Probability			
Impact			
Timeframe	Origin	Class	Assigned to:
Context			
Mitigation Strategy			
Contingency Plan and Trigger			
Status			Status Date
Approval	Closing Date __/__/__	Closing Rationale	

Evaluating Attributes of Risk

Purpose:
to gain a better understanding of the risk by determining the expected impact, probability, and timeframe of a risk

Description - involves establishing values for:

***Impact*: the loss or effect on the project if the risk occurs**
***Probability*: the likelihood the risk will occur**
***Timeframe*: the period when you must take action to mitigate the risk**

Levels of Analysis

Level	*Impact*	*Probability*	*Timeframe*
binary level	significant insignificant	likely not likely	near far
tri-level	high moderate low	high moderate low	near mid far
5-level	very high high moderate low very low	very high high moderate low very low	imminent near mid far very far
n-level	n levels of impact	n levels of probability	n levels of timeframe

Example -
Tri-Level Attribute Evaluation

Each attribute has one of three values

- **Impact: catastrophic, critical, marginal**
- **Probability: very likely, probable, improbable**
- **Timeframe: near-term, mid-term, far-term**

Risk Exposure

		Probability		
		Very Likely	Probable	Improbable
Impact	Catastrophic			Moderate
	Critical		Moderate	Low
	Marginal	Moderate	Low	Low

Example: NASA Safety Impact Definitions

Catastrophic

- **loss of entire system**
- **loss of human life**
- **permanent disability**

Critical

- **major system damage**
- **severe injury**
- **temporary disability**

Marginal

- **minor system damage**
- **minor injury (e.g., scratch)**

Negligible

- **no system damage**
- **no injury (possibly some aggravation)**

Example - Impact Definitions

	Catastrophic	Critical	Marginal
Schedule slip	> 20%	10 – 20%	0 – 10%
Cost overrun	> 25%	10 – 25%	0 – 10%
Failure	System is lost	Major function lost	Data lost

Example Timeframe Definitions

A risk is *near-term* if the project must take action or will be impacted by the risk in the next 90 days.

A risk is *mid-term* if the project must take action or will be impacted by the risk in the next 90-180 days.

A risk is *far-term* if the project need not take action or will not be impacted by the risk in the next 180 days.

Example Probability Definitions

A risk is *very likely* if there is a >70% probability that it will occur.

A risk is *probable* if there is a 30-70% probability that it will occur.

A risk is *improbable* if there is a <30% probability that it will occur.

Exercise

Tri-Level Attribute Evaluation

Criteria and Attributes for IR-SIP

Jerry Johnstone's criteria for what's currently important to the project:

- must meet the schedule
- can't delete any of the technical or performance requirements
- must keep to the budget (Jerry knows there's a small amount of slack in the budget, but he doesn't want the project personnel to know.)

Attribute	Value	Description
Probability	Very Likely (H)	High chance of this risk occurring, thus becoming a problem >70%
	Probable (M)	Risk like this may turn into a problem once in a while 30% < x < 70%
	Improbable (L)	Not much chance this will become a problem 0% < x < 30%
Impact	Catastrophic (H)	Loss of IR-SIP; unrecoverable failure of IR-SIP operations; major system damage to IR-SIP; schedule slip that causes vehicle launch date to be missed; cost overrun exceeding 50% of planned costs.
	Critical (M)	Minor system damage to IR-SIP with recoverable operational capacity; cost overrun exceeding 10% (but less than 50%) of planned costs.
	Marginal (L)	Minor system damage to IR-SIP; recoverable loss of IR-SIP operational capacity; internal schedule slip that does not impact vehicle launch date; cost overrun of less than 10% of planned costs.
Timeframe	Near-term (N)	Note: Refers to *when* action must be taken on the risk. In the next month
	Mid-term (M)	1-2 months from now
	Far-term (F)	3 or more months from now

Case Study

Tri-level Attribute Evaluation

Case Study Setting: It is October 20, 1995. The IR-SIP project is behind schedule in completing the Systems Requirements and Design. These are running in parallel. Both the IR-SIP Flight and the Mission Software have started requirements definition. The Science requirements are still incomplete and the AA Interface requirements are behind schedule.

Key: Using the IR-SIP criteria description, evaluate each risk with respect to:

Attribute	Value	Description
Probability	Very Likely (H)	High chance of this risk occurring, thus becoming a problem >70%
	Probable (M)	Risk like this may turn into a problem once in a while 30% < x < 70%
	Improbable (L)	Not much chance this will become a problem 0% < x < 30%
Impact	Catastrophic (H)	Loss of IR-SIP; unrecoverable failure of IR-SIP operations; major system damage to IR-SIP; schedule slip that causes vehicle launch date to be missed; cost overrun exceeding 50% of planned costs.
	Critical (M)	Minor system damage to IR-SIP with recoverable operational capacity; cost overrun exceeding 10% (but less than 50%) of planned costs.
	Marginal(L)	Minor system damage to IR-SIP; recoverable loss of IR-SIP operational capacity; internal schedule slip that does not impact vehicle launch date; cost overrun of less than 10% of planned costs.
Timeframe	Near-term (N)	Note: Refers to *when* action must be taken on the risk. In the next month
	Mid-term (M)	1-2 months from now
	Far-term (F)	3 or more months from now

Risk ID	Risk Statement	Probability	Im-pact	Time-frame
1	This is the first time that the software staff will use OOD; The staff may have a lower-than-expected productivity rate and schedules may slip because of the associated learning curve.			
2	Commercial parts suitability for space applications is unknown; parts failure may lead to system failure and use of space grade parts may cause schedule delays since space qualified parts procurement have a procurement lead time of at least 18 months.			
3	The high-speed fiber optic data bus is untested technology; the bus will not perform as specified and high data transfer rates will not be sustained.			
4	First time the IR Instrument Project manager is managing a project to go into space; Project may fail due to insufficient / poor management.			
5	Lack of a thorough hardware test program; mission failure due to environmental conditions not tested.			
6	Project software schedule and resources were underestimated; Schedule slips, cost overruns, and a reduction in adequate testing time are likely results.			

Tri-Level Attribute Evaluation

Setting: October 20th, the IR-SIP project is behind schedule in completing the Systems requirements and Design. These are running in parallel. Both the Flight and Mission segments have started requirements definition. The Science requirements are still incomplete and the AA interface requirements are behind schedule.

Risk ID	Risk Statement	Probability	Impact	Time-frame
1	This is the first time that the software staff will use OOD; The staff may have a lower-than-expected productivity rate and schedules may slip because of the associated learning curve.			
2	Commercial parts are being selected for space flight applications and their suitability to meet environmental conditions is unknown; these parts may fail to operate on-orbit within the environment window, leading to system level failures. Also, environmental testing of these parts can be expensive and cause schedule delays.			
3	The high-speed fiber optic data bus is untested technology; the bus will not perform as specified and high data transfer rates will not be sustained.			
4	First time the IR Instrument Project manager is managing a project to go into space; Project may fail due to insufficient / poor management.			
5	Lack of a thorough hardware test program; mission failure due to environmental conditions not tested.			
6	Project software schedule and resources were underestimated; Schedule slips, cost overruns, and a reduction in adequate testing time are likely results.			

Classifying Risks

Purpose:
- look at a set of risks and how those risks relate to each other within a given structure
- efficiently sort through large amounts of data

Description:

involves grouping risks based on shared characteristics. The groups or classes show relationships among the risks.

Classification Perspectives

<u>By Source:</u> Risks are grouped based on the same source or root cause. This will show the major sources of risk to the project.

<u>By Impact:</u> Risks are grouped based on where or how the impact will be felt by the project. This shows the major aspects of the project that are most at risk.

Example IR-SIP Classification of Risk - 1

By Source of Risk - <u>Management Process</u>

ID	Risk Statement
4	First time the IR Instrument Project manager is managing a project to go into space; Project may fail due to insufficient / poor management.
6	Project software schedule and resources were underestimated; Schedule slips, cost overruns, and a reduction in adequate testing time are likely results.
9	Lack of an adequate configuration management system; Inability to track parts and materials in case of GIDEP alerts.
12	Resource availability estimates were overly optimistic- schedule shows all resources are available at the start of each WBS element; schedule slips, cost overruns, and reduction in adequate testing time are likely.

Example IR-SIP Classification of Risk - 2

By Impact of Risk

	CI 5.1 IR-SIP Hardware
5	Lack of a thorough hardware test program; mission failure due to environmental conditions not tested.
8	Mission objectives require the use of new technology in an instrument's detector circuit. The selected approach involves scaling down existing technology to operate at higher frequencies. Manufacturability and survivability of the more delicate part is unproven. Problems in either of these areas may result in schedule delay, cost overruns, or a shortened mission life.
19	Ability of new hardware to meet sampling rate timing requirements is unknown; failure to meet sample rate requirements could result in loss of science data and we may need alternative hardware or be forced to accept decreased software performance requirements.
	CI 5.2 IR-SIP Software
1	This is the first time that the software staff will use OOD; The staff may have a lower-than-expected productivity rate and schedules may slip because of the associated learning curve.
4	First time the IR Instrument Project manager is managing a project to go into space; Project may fail due to insufficient / poor management.
13	Waterfall lifecycle model is being used to develop all IR-SIP software; it may cause serious integration problems between IR-SIP CI and IR sensor and/or between IR-SIP CI and AA platform leading to a missed launch window, excessive cost to meet window, or failure to successfully integrate the system.

Dealing With Sets of Risks

During classification, it may be decided that some risks should be mitigated and tracked as a set. When this happens

- create a summary risk statement
- assign new ID but maintain linkages to original risks
  - keep all context
  - move individual risk statements and ID #s to context
- keep the worst-case impact, probability, and timeframe attribute evaluations
- update database

Example - Consolidating Risks

		Probability	Impact	Time-frame
101	Use of C++, the selected compiler, and OOD are new for software staff; decreased productivity due to unexpected learning curves may cause coding schedule to slip.	H	M	N
1	This is the first time that the software staff will use OOD; The staff may have a lower-than-expected productivity rate and schedules may slip because of the associated learning curve.	H	M	N
16	The C++ compiler selected for use does not come with very good user documentation, as supplied by the vendor; decreased productivity likely as software developers stumble over the same problems.	M	M	M
17	This is the first time that software staff has used C++; staff may have lower-than-expected productivity rate, schedules may slip.	M	M	M

Prioritizing Risks

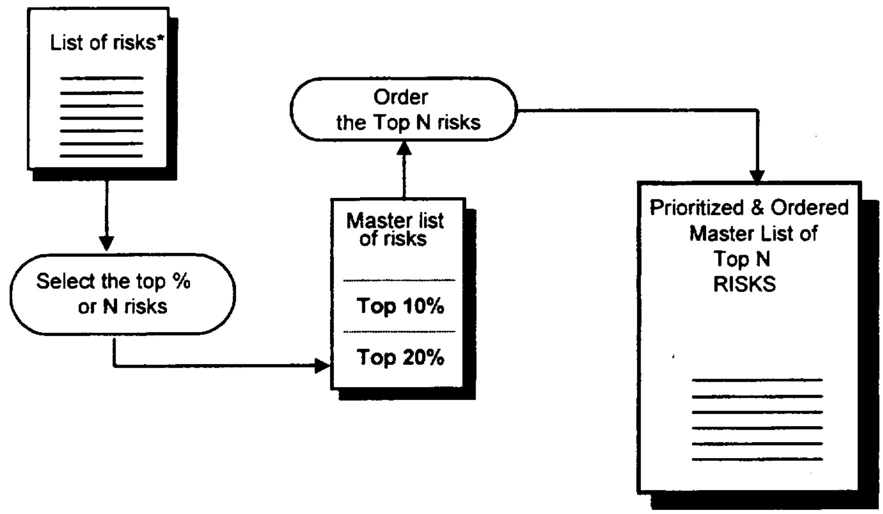
Purpose:

- sort through a large amount of risks and determine which are most important
- separate out which risks should be dealt with first (the vital few risks) when allocating resources

Description:

- involves partitioning risks or groups of risks based on the Pareto "vital few" sense and ranking risks or sets of risks based upon a criterion or set of criteria

Two Step Risk Prioritization



Example Pareto Top 20%

			Prob-ability	Impact	Time-frame
	2	Commercial parts are being selected for space flight applications and their suitability to meet environmental conditions is unknown; these parts may fail to operate on-orbit within the environment window, leading to system level failures. Also, environmental testing of these parts can be expensive and cause schedule delays.	H	H	M
10%	5	Lack of a thorough test program; mission failure due to environmental conditions not tested.	H	H	F
	100	Project resources (personnel number and availability) and schedules were underestimated; schedule slips, cost overruns, reduction in adequacy of development processes (especially testing time adequacy) likely.	H	H	N
	101	Use of C++, the selected compiler, and OOD are new for software staff; decreased productivity due to unexpected learning curves may cause coding schedule to slip.	H	M	N
20%	10	Yearly congressional NASA budget profiles are subject to change; this may cause the project funding profile to change each year with associated replanning, schedule impacts, labor cost increases, loss of key personnel, or project termination.	H	M	F
	4	First time the IR Instrument Project manager is managing a project to go into space; Project may fail due to insufficient / poor management.	M	H	N
	7	Science requirements have substantial TBDs; late completion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.	M	H	M

Cut off point for top risk listing based on Project concerns

Prioritization Criteria

The criterion or set of criteria used to rank the risks is chosen based on what's most important to the project.

Recall IR-SIP example:

- **must meet the schedule**
- **can't delete any of the technical or performance requirements**
- **must keep to the budget**

Exercise

Multivoting

Exercise - Multivoting

	Risk:											
Evaluator	A	B	C	D	E	F	G	H	I	J	K	L
Eval1	3		1					2				
Eval2		3						2		1		
Eval3	2		1					3				
Eval4	1	2						3				
Eval5		2	1					3				
TOTAL	6	7	3					13		1		

Example:
5 participants
12 risks
3 weighted votes (1 2 3)

Risk order of criticality:
H B A C J

Exercise - Multivoting

Risks	2	5	100	101	10	4	7	14	18	20
Eval1										
Eval2										
Eval3										
Eval4										
Eval5										
TOTAL										

Case Study EXERCISE - Multivoting Form

Directions: It is October 20, 1995. Jerry Johnstone, R.C.Everette, W. Peacock, and C. White have come together to prioritize the risks on the Top N list (which were selected using the Pareto Top N Method). Review the risk statements and context with respect to the prioritization criteria

- **must meet the schedule**
- **can't delete any of the technical or performance requirements**
- **must keep to the budget**

Vote for the three risks that are most important to the project based on the prioritization criteria. Give the most important risk 3 points, the next most important risk 2 points, and give the third most important risk 1 point.

Risk ID	Risk Statement	Points
2	Commercial parts are being selected for space flight applications and their suitability to meet environmental conditions is unknown; these parts may fail to operate on-orbit within the environment window, leading to system level failures. Also, environmental testing of these parts can be expensive and cause schedule delays.	
5	Lack of a thorough hardware test program; mission failure due to environmental conditions not tested.	
100	Project resources (personnel number and availability) and schedules were underestimated; schedule slips, cost overruns, reduction in adequacy of development processes (especially testing time adequacy) likely.	
101	Use of C++, the selected compiler, and OOD are new for software staff; decreased productivity due to unexpected learning curves may cause coding schedule to slip.	
10	Yearly congressional NASA budget profiles are subject to change; this may cause the project funding profile to change each year with associated replanning, schedule impacts, labor cost increases, loss of key personnel, or project termination.	
4	First time the IR Instrument Project manager is managing a project to go into space; Project may fail due to insufficient / poor management.	
7	Science requirements have substantial TBDs; late completion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.	
14	Contracting a different test facility for acoustical testing; parts may be insufficiently tested or parts may be damaged with excessive testing.	
18	There is no AA Satellite Simulator currently scheduled for development; probable that the IR-SIP CSCI will fail when initially integrated with the actual AA Satellite since prior interface testing will not have been possible, thus fixes will be done very late in the project schedule and may cause the launch date to slip.	
20	Subset of IR Post Processing CSCI requirements is to be satisfied with COTS products; Integration time and lifecycle costs may increase from original estimates which assumed significant saving from COTS use, leading to schedule slips and cost overruns.	

Comparison Risk Ranking

Compare two risks at a time with respect to the project criteria.

IR-SIP example: Which risk is more important? (i.e., may cause the project to
- **not meet the schedule**
- **delete a technical or performance requirement**
- **not keep to the budget**

(2) Commercial parts are being selected for space flight applications and their suitability to meet environmental conditions is unknown; these parts may fail to operate on-orbit within the environment window, leading to system level failures. Also, environmental testing of these parts can be expensive and cause schedule delays.

OR

(5) Lack of a thorough hardware test program; mission failure due to environmental conditions not tested.

Analysis Summary - 1

Evaluate:
- impact (I)
- probability (P)
- timeframe (T)

Risk	I	P	T
Risk a	M	M	F
Risk b	M	L	N
Risk c	L	H	N
. . .			

Consolidate risks

Classify:
- identify duplicates
- consolidate risks to sets

Risk	I	P	T
Risk set A	H	M	F
——			
Risk b	M	L	N
Risk c	L	H	N
. . .			

Sort by evaluation results

Prioritize:
- identify Pareto top N
- rank top N

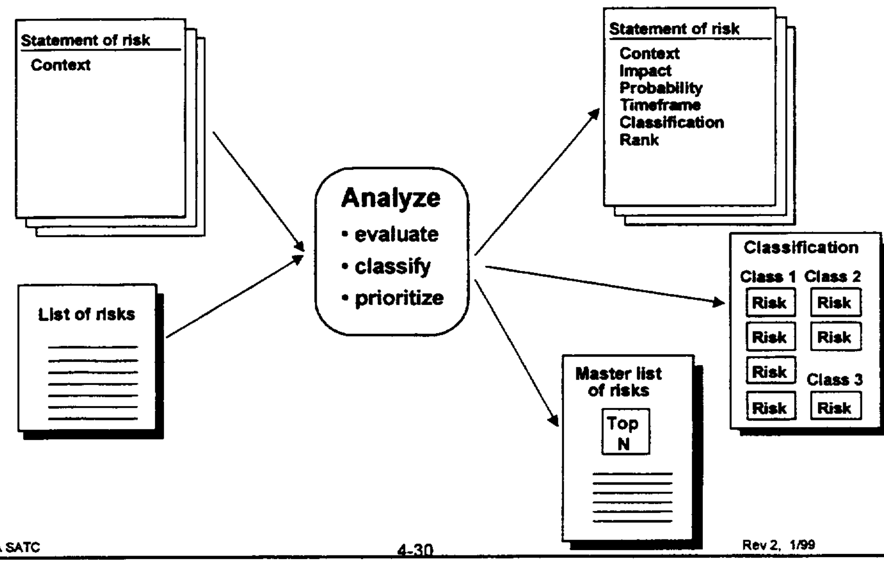
Pareto top N

Risk	I	P	T
Risk n	H	H	N
Risk s	H	M	N
Risk set A	H	M	F
——			
Risk c	L	H	N

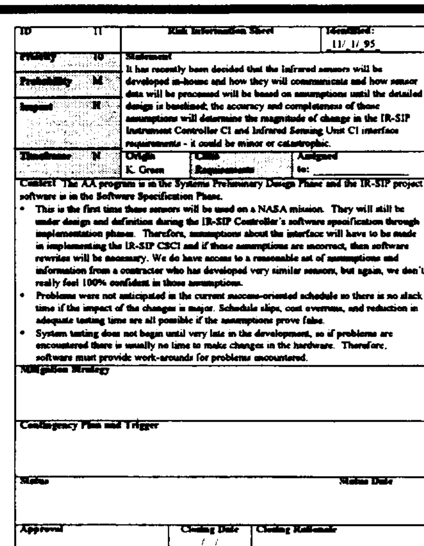
Rank order the Pareto top N

Top N
1.
2.
3.
. . .

Analysis Summary - 2



Risk Information Sheet after Analyze



ID 11	Risk Information Sheet		Identified: 11/ 1/ 95
Priority 10	Statement It has recently been decided that the Infrared sensors will be developed in-house and how they will communicate and how sensor data will be processed will be based on assumptions until the detailed design is baselined; the accuracy and completeness of those assumptions will determine the magnitude of change in the IR-SIP Instrument Controller CI and Infrared Sensing Unit CI interface requirements - it could be minor or catastrophic.		
Probability M			
Impact H			
Timeframe N	Origin K. Green	Class Requirements	Assigned to:
Context The AA program is in the Systems Preliminary Design Phase and the IR-SIP project software is in the Software Specification Phase. • This is the first time these sensors will be used on a NASA mission. They will still be under design and definition during the IR-SIP Controller's software specification through implementation phases. Therefore, assumptions about the interface will have to be made in implementing the IR-SIP CSCI and if these assumptions are incorrect, then software rewrites will be necessary. We do have access to a reasonable set of assumptions and information from a contractor who has developed very similar sensors, but again, we don't really feel 100% confident in those assumptions. • Problems were not anticipated in the current success-oriented schedule so there is no slack time if the impact of the changes is major. Schedule slips, cost overruns, and reduction in adequate testing time are all possible if the assumptions prove false. • System testing does not begin until very late in the development, so if problems are encountered there is usually no time to make changes in the hardware. Therefore, software must provide work-arounds for problems encountered.			
Mitigation Strategy			
Contingency Plan and Trigger			
Status			Status Date
Approval	Closing Date / /	Closing Rationale	

Case Study

Risk Information Sheet After Analysis

<table>
<tr><td>ID 11</td><td colspan="2">Risk Information Sheet</td><td>Identified:
11/ 1/ 95</td></tr>
<tr><td>Priority 10
Probability M
Impact H</td><td colspan="3">Statement
It has recently been decided that the Infrared sensors will be developed in-house and how they will communicate and how sensor data will be processed will be based on assumptions until the detailed design is baselined; the accuracy and completeness of those assumptions will determine the magnitude of change in the IR-SIP Instrument Controller CI and Infrared Sensing Unit CI interface requirements - it could be minor or catastrophic.</td></tr>
<tr><td>Timeframe N</td><td>Origin
K. Green</td><td>Class
Requirements</td><td>Assigned to: ______</td></tr>
<tr><td colspan="4">Context The AA program is in the Systems Preliminary Design Phase and the IR-SIP project software is in the Software Specification Phase.
• This is the first time these sensors will be used on a NASA mission. They will still be under design and definition during the IR-SIP Controller's software specification through implementation phases. Therefore, assumptions about the interface will have to be made in implementing the IR-SIP CSCI and if those assumptions are incorrect, then software rewrites will be necessary. We do have access to a reasonable set of assumptions and information from a contractor who has developed very similar sensors, but again, we don't really feel 100% confident in those assumptions.
• Problems were not anticipated in the current success-oriented schedule so there is no slack time if the impact of the changes is major. Schedule slips, cost overruns, and reduction in adequate testing time are all possible if the assumptions prove false.
• System testing does not begin until very late in the development, so if problems are encountered there is usually no time to make changes in the hardware. Therefore, software must provide work-arounds for problems encountered.</td></tr>
<tr><td colspan="4">Mitigation Strategy</td></tr>
<tr><td colspan="4">Contingency Plan and Trigger</td></tr>
<tr><td colspan="3">Status</td><td>Status Date</td></tr>
<tr><td>Approval
______</td><td>Closing Date
__/__/__</td><td colspan="2">Closing Rationale</td></tr>
</table>

Key Points - 1

Evaluate risks at a level that is sufficient to determine the relative importance

Select attribute definitions (e.g. catastrophic impact) that make sense for your project.

Classify risks to help the project understand the risks.

Group related risks into sets to help build more cost-effective mitigation plans.

Key Points - 2

Prioritize to determine which risks should be dealt with first when allocating resources.

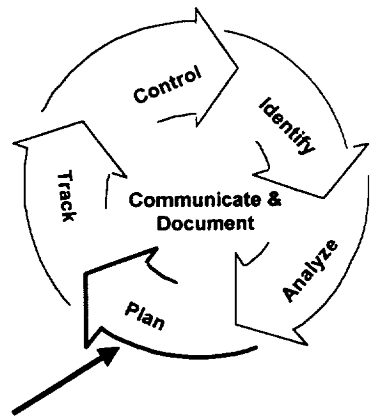
Prioritize the risks based on the criteria for what is most important to the project.

Communication is central to:

- defining project evaluation definitions
- evaluating risks
- selecting a project classification scheme
- classifying risks
- defining prioritization criteria
- identifying and prioritizing the top N risks

Module 5

Plan



Overview

Planning activities overview

Planning activities
- assigning responsibility
- determining approach
- defining scope and actions

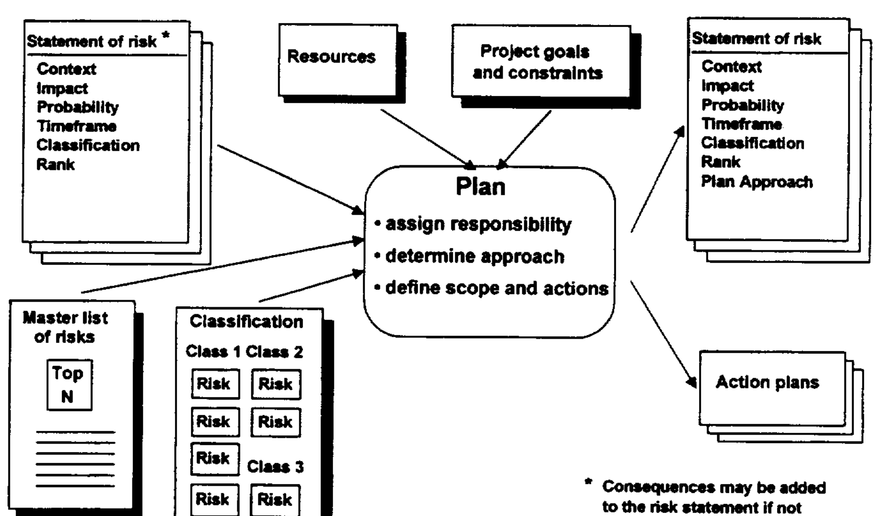
Mitigating a set of related risks

What Is Planning?

Planning is the function of deciding what, if anything, should be done with a risk.

Planning answers the questions
- **Is it my risk? (responsibility)**
- **What can I do? (approach)**
- **How much and what should I do? (scope and actions)**

Planning Activities Overview



* Consequences may be added to the risk statement if not already documented

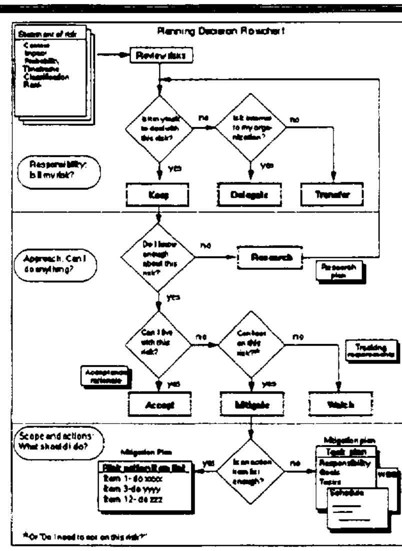
Risk Information Sheet

To be completed:

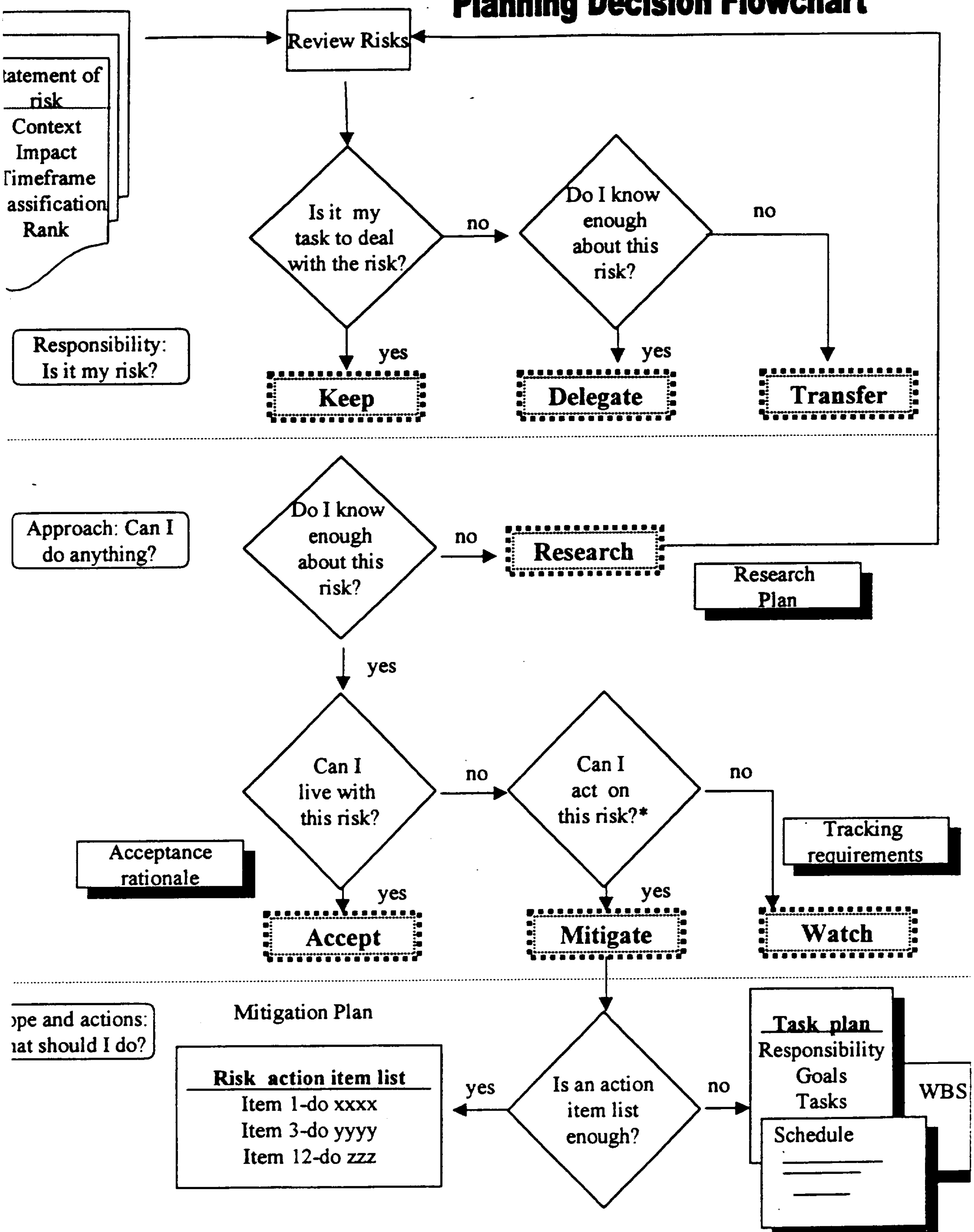
- Assigned to
- Mitigation Strategy
- Contingency plan and trigger

ID	Risk Information Sheet	Identified: / /
Priority Probability Impact Timeframe	Statement	
	Origin | Class	[redacted]
Context		
[redacted]		
Status		Status Date
Approval	Closing Date / /	Closing Rationale

Planning Decision Flowchart



Planning Decision Flowchart



*Or "Do I need to act on this risk?"

Project Considerations

What is currently important to the project, management, customer, or user?

Are there critical milestones the project is currently facing?

What limits and constraints do the project, organization, group, or manager have?

What milestones and limits are fixed? flexible?

What resources are available for mitigation?

How does this risk fit into the overall project issues and concerns? When is the best time to address or mitigate a risk?

Assigning Responsibility

Purpose:

- ensure that no risks are ignored
- make effective use of expertise and knowledge within the project when planning for risk mitigation
- ensure that risks are being managed by those with the appropriate abilities, knowledge, and authority to commit resources for mitigation

Description:

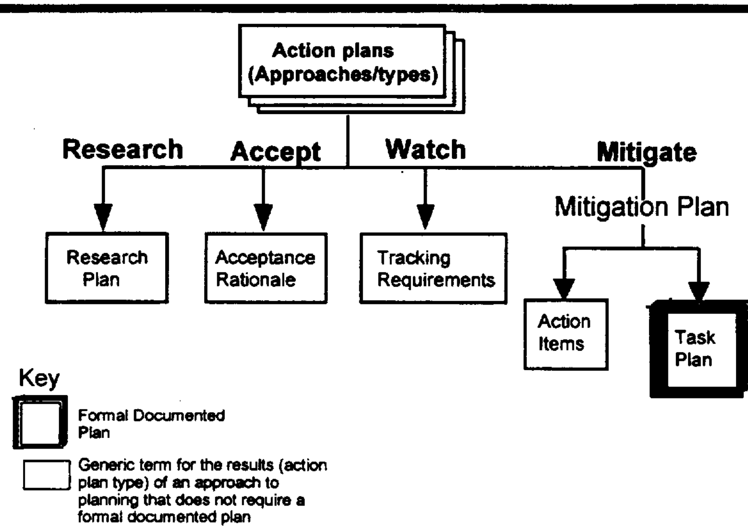
- involves reviewing the risk(s) and determining who is best able to deal with the risk(s)

Determining Approach

Purpose:
- ensure you know enough to make an informed decision
- pick an appropriate approach for effective management of the risk(s)
- establish measurable mitigation goals that provide a target for evaluating success and direction during the development of action plans

Description:
- involves reviewing the risk(s) and determining the best approach to take

Action Plan Approaches



Action #1 - Research

Investigate the risk until you know enough to be able to decide
- if it is still your responsibility
- what to do about it (accept, watch, or mitigate)

Risk action plan type
- research plan

Action #2 - Accept

Do nothing. The risk will be handled as a problem if it occurs. No further resources are expended managing the risk.

Risk action plan type
- acceptance rationale

Action #3 - Watch

Monitor the risks and their attributes for early warning of critical changes in impact, probability, timeframe, or other aspects.

Risk action plan type
- tracking requirements*

*Tracking requirements include indicators for monitoring the risk, triggers, or thresholds for taking action, and reporting requirements (e.g., how often, by whom, extent of the report, and when).

Action #4 - Mitigate

Eliminate or reduce the risk by
- reducing the impact
- reducing the probability
- shifting the timeframe

Risk action plan type
- mitigation plan (action item list or task plan)
- tracking requirements

Discussion - Determining Approach

Risk ID	Risk Statement	Assigned To:	Plan	Rationale
7	Science requirements have substantial TBDs; late completion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.	Johnstone		
13	Waterfall lifecycle model is being used to develop all IR-SIP software; it may cause serious integration problems between IR-SIP CI and IR sensor and/or between IR-SIP CI and AA platform leading to a missed launch window, excessive cost to meet window, or failure to successfully integrate the system.	Everette		
15	The funding and development schedule for the AA satellite is subject to change; IR-SIP schedule slips, cost overruns, and a reduction in adequate testing time are likely as unscheduled changes will have to be made to the software to match AA project changes.	Johnstone		
20	Subset of IR Post Processing CSCI requirements is to be satisfied with COTS products; Integration time and lifecycle costs may increase from original estimates which assumed significant saving from COTS use, leading to schedule slips and cost overruns.	Everette		

Contingency Plans

Not all mitigation plans can or should be carried out immediately, for example:

- there may not be sufficient funding at this time
- other circumstances (such as having the right personnel) may not be right
- it may be a low probability, catastrophic impact risk with an expensive mitigation plan

May be used as Plan B if Plan A fails

Contingency plans are held in reserve until specific conditions are true or certain events occur

- watch for the conditions and events!

Defining Scope and Actions

Purpose:
- take a balanced approach in developing effective actions to mitigate risks

Description:
- involves reviewing the risk(s) and determining the appropriate level of mitigation to take and the goal of the mitigation

Which Type of Mitigation Action?

What criteria are used to determine when to use action item lists and task plans?

- relative importance of the risk(s)
- complexity of the issues
- breadth of expertise required to develop mitigation strategies
- probability and impact of the risk (particularly catastrophic)
- available planning resources (particularly personnel)

Action Item List vs. Task Plan

Action Item List	Task Plan
Risk statement(s)	Risk statement(s)
Mitigation goal/ success measures	Mitigation goal/ success measures
Responsible person	Responsible person(s)
	Related Risks
	Due date for task plan completion
Action items	Chosen strategy(ies)
	Specific actions
	Budget
Due dates and closing date	Schedule (e.g., Gantt or PERT charts)
	Risk tracking indicators, thresholds, reporting frequency
(Optional) contingency action and trigger	Contingency strategy, actions, and trigger

Task Plan Components

Risks

Related risks

Specific actions to take

Strategy(ies)

Cost of strategy/actions

Staff roles & responsibilities

Risk tracking requirements

Due dates & schedules

Success criteria

Mitigation goals

Contingency strategy and triggers

Example

Task Plan

Discussion - Defining Scope & Actions

Risk ID	Risk Statement	Assigned to	Plan: Determine scope results	Rationale
11	It has recently been decided that the Infrared sensors will be developed in-house and how they will communicate and how sensor data will be processed will be based on assumptions until the detailed design is baselined; the accuracy and completeness of those assumptions will determine the magnitude of change in the IR-SIP Instrument Controller CI and Infrared Sensing Unit CI interface requirements – it could be minor or catastrophic.	Jonhstone		
7	Science requirements have substantial TBDs; late ompletion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.	Johnstone		

Case Study

Task Plan

Responsible Person: J. Johnstone (for approval); R.C. Everette (for recommendations and implementation)

Last Updated: 6/7/96

Origination date: 3/4/96

Risk Statement

Risk # 7

Science requirements have substantial TBDs; late completion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.

Classification: Requirements

Related risks: None

Identified causes

- inadequate scheduling to allow for requirements definition
- inadequate civil service and contractor personnel resource planning
- all of the science requirements are still not available

Mitigation goals/success measures/criteria

The goal of this task plan is to

Complete the science requirements and submit the change for implementation WITHOUT slipping the overall development completion date. It is preferable to not use overtime or additional resources.

Chosen Strategies

The selected strategies to address the key causes and to reach the mitigation goal are

- to analyze, research, and complete the TBD science requirements, and to submit change requests
- to reprioritize the baselined requirements and reorder the builds to minimize impact of TBDs

Specific actions

The following work breakdown structure (WBS) describes the actions that will be performed as part of the mitigation plan and identifies who is responsible for completing them. This information will also be reflected in a Gantt chart.

1.0 Reprioritize the baselined requirements and reorganize the builds to implement the high priority requirements first. The likelihood of their changing will be factored into the prioritization process. (J. Johnstone)

   1.1 Identify requirements with high probability of change. (R. C. Everette)

   1.2 Identify critical path dependencies among requirements and software modules. (R. C. Everette)

   1.3 Build a prioritized list of requirements. (R. C. Everette)

   1.4 Reorganize the contents and schedule of builds to meet the new priorities. (R. C. Everette)

   1.5 Distribute the changes in build content and schedule to all personnel, and tell the customers that no changes to a specific build will be accepted once implementation of that build has begun (except for corrections to requirements errors that would cause mission failure). (J. Johnstone)

2.0 Estimate the impact to the schedule for builds and requirements based on the projected completion of the TBD requirements. Verify (as much as possible) that the new schedule accounts for the anticipated changes. (R. C. Everette)

3.0 Complete the requirements document for TBD Requirements 38-42 and submit a change request. (John Smith/NASA)

   3.1 Estimate the intermediate completion milestones.

   3.2 Report progress weekly.

   3.3 Complete peer review requirements.

   3.4 Submit change requests upon the completion of the requirements.

4.0 Complete the requirements document for TBD Requirement 73 and submit a change request. (John Smith/NASA)

   4.1 Estimate the intermediate completion milestones.

   4.2 Report progress weekly.

   4.3 Complete peer review requirements.

   4.4 Submit a change request upon the completion of the requirements.

5.0 Complete the requirements document for TBD Requirement 104 and submit a change request. (Mary Blue/NASA)

   5.1 Estimate the intermediate completion milestones.

   5.2 Report progress weekly.

   5.3 Complete peer review requirements.

   5.4 Submit a change request upon the completion of the requirements.

6.0 Complete the requirements document for TBD Requirements 143-149 and submit a change request. (Joe Kelley/University Intern)

   6.1 Estimate the intermediate completion milestones.

   6.2 Report progress weekly.

   6.3 Complete peer review requirements.

   6.4 Submit change requests upon the completion of the requirements.

7.0 Set up a tracking mechanism for change requests and help R. C. Everette determine the magnitude of the problem created by change requests. Weekly reports will be provided to R. C. Everette. The reports will include the impact to the schedule and the resources required to implement each submitted change. (J. Johnstone)

   7.1 Design a weekly status report.

   7.2 Set up automated metrics collection and reporting.

Risk tracking indicators

TBD requirements completion:

Indicator: actual completion dates compared to planned completion dates

Trigger: a projected 10% schedule slip in the completion of any requirements document is cause for review

Trigger: a projected 25% schedule slip in the completion of any requirements document will trigger contingency plan A

Change request magnitude

Indicator: the cumulative schedule impact due to the changes (based on submitted change requests)

Indicator: the cumulative resource requirements required to implement the changes (based on submitted change requests)

Trigger: If either the cumulative schedule impact indicator or the cumulative resource requirements indicator exceeds their projections by 20%, it will trigger contingency plan B

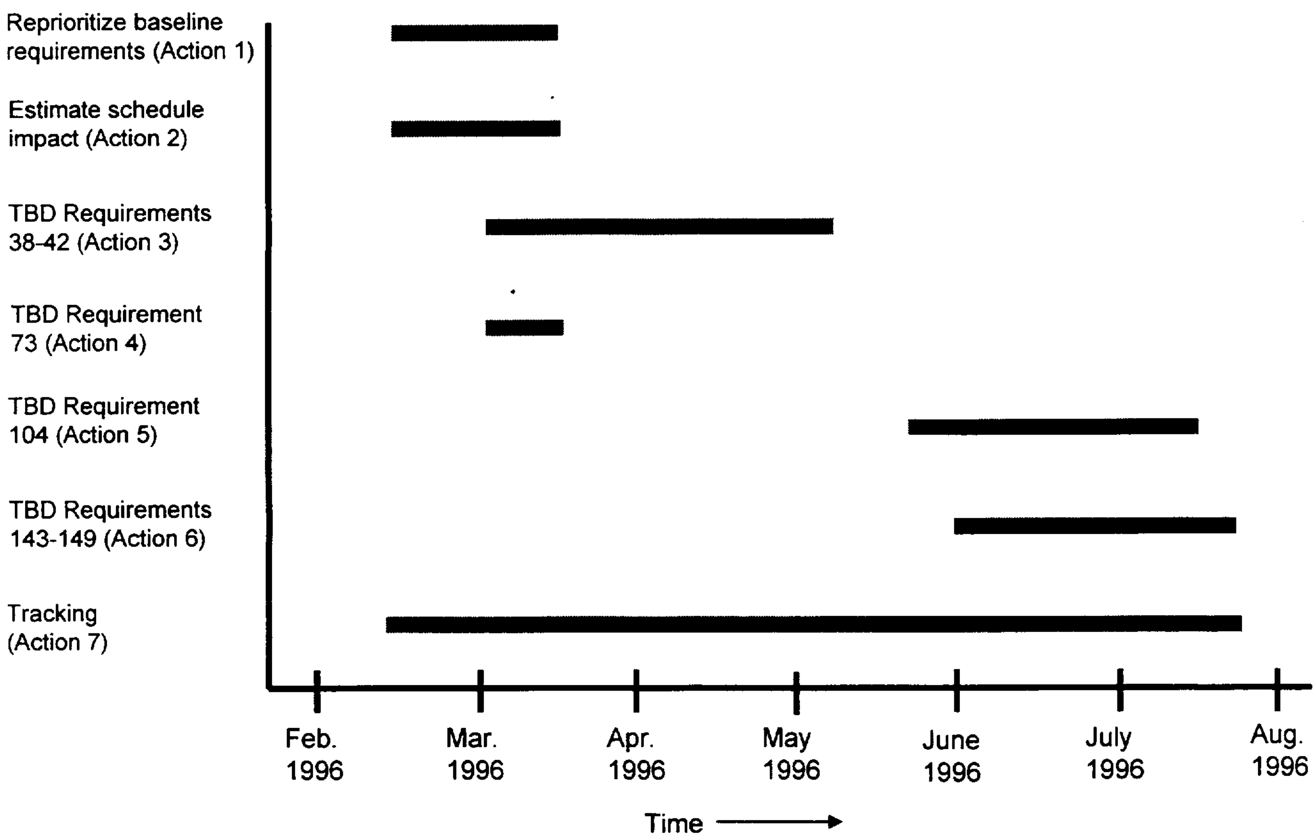
Budget

- Planning/oversight:
  J. Johnstone/R. C. Everette: 5 days
- Completing TBD requirements:
  3 civil servants: 14 weeks
  1 university intern: 7 weeks, $10,000
- Reprioritizing:
  R. C. Everette: 7 days
  2 team members: 1 day each to review
- Tracking costs:
  1 civil servant: 3 days to set up automated system;
  R. C. Everette & J. Smith: 2 days each to determine tracking measures, triggers, report format, and intermediate triggers. (Cost to produce weekly reports is negligible)
- Totals:
  Civil service time: 18-person weeks
  University Intern cost: $10,000

Expected return: The number of errors is projected to decrease by approximately 75%. The amount of resources assigned to late requirements changes should decrease accordingly by 75%. For this project, the total estimated savings is 50% of the total planned budget. The probability for mission failure due to this risk will be eliminated.

Schedule (Gantt chart)

Action	Start Date	End Date
1	February 15, 1996	March 15, 1996
2	February 15, 1996	March 15, 1996
3	March 1, 1996	May 7, 1996
4	March 1, 1996	March 15, 1996
5	May 24, 1996	July 15, 1996
6	June 1, 1996	July 21, 1996
7	February 15, 1996	July 21, 1996



Contingency strategies, actions, and triggers

Contingency Plan A:

Trigger:	A projected 25% schedule slip in the completion of any requirements document
Strategy/actions:	Authorize contractor overtime to assist civil service (a maximum of 10 person weeks in contractor time is allowed). Approval by J. Johnstone is required.

Contingency Plan B:

Trigger:	When either the cumulative schedule impact indicator or the cumulative resource requirements indicator exceeds its projections by 20%
Strategy/actions:	Drop the lower-level science requirements to compensate for the estimated development time required to complete the higher-priority requirements.

Mitigation Goals and Success Measures

Set a realistic, measurable (or verifiable) goal for mitigating the risk, for example
- avoid any changes to scheduled milestones
- eliminate change requests unsupported by funding to implement the change

Define success criteria— you need to know when you've succeeded or failed

For example
- all current change requests implemented by 3/1/96 with no change to scheduled milestones

Discussion - Goals & Success Measures

Risk 7 - Science requirements have substantial TBDs; late completion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.

What Goals & Success measures would you look for?

Discussion - Goals & Success Measures

Risk 14 - Contracting a different test facility for acoustical testing; parts may be insufficiently tested or parts may be damaged with excessive testing.

What Goals & Success measures would you look for here?

Example - Mitigation Planning Worksheet

Planning Worksheet	
Risk ID 7	Responsibility J. Johnson
Risk statement Science requirements have substantial TBDs; late completion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.	
Mitigation goals and constraints (in observable terms) Science requirements must be completed and all related change requests submitted for implementation. No slipping of the overall development completion date is allowed. Preferable to not use overtime or additional resources but if necessary to keep completion date, do so.	
Additional data (e.g., root causes, impacted elements)	
Related risks	
Alternative strategies/actions	Estimated costs
Related mitigation plans	
Strategy evaluation criteria	
Chosen strategy/actions	Success measures
Contingency strategy	Contingency trigger

Case Study

Planning Worksheet

Planning Worksheet	
Risk ID 7	**Responsibility:** J. Johnstone
Risk statement Science requirements have substantial TBDs; late completion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.	
Mitigation goals and constraints (in observable terms) Science requirements must be completed and all related change requests submitted for implementation. No slipping of the overall development completion date is allowed. Preferable to not use overtime or additional resources but if necessary to keep completion date, do so.	
Additional data (e.g., root causes, impacted elements)	
Related risks	
Alternative strategies/actions	**Estimated costs**
Related mitigation plans	
Strategy evaluation criteria	
Chosen strategy/actions	**Success measures**
Contingency strategy	**Contingency trigger**

Planning for Risk Sets

Mitigation goals can be hierarchical.

The planning focus should be on high-priority or Top N risks in the set.

Monitoring a set of risks usually requires a set of indicators.

Mitigating a Set of Related Risks- 1

Purpose:

- increase the cost effectiveness of mitigation plans by eliminating duplicate efforts
- avoid conflicting mitigation goals and actions
- integrate planning efforts and avoid unnecessary time developing plans

Mitigating a Set of Related Risks- 2

Questions to consider:

- Is there a set of risks that would benefit from coordinated mitigation?
- Do we know enough about these risks to proceed?
- What are the goals of mitigating this set of risks?
- What strategies will address these risks?
- What indicators are needed for monitoring a set of risks?

Summary of Action Plan Approaches

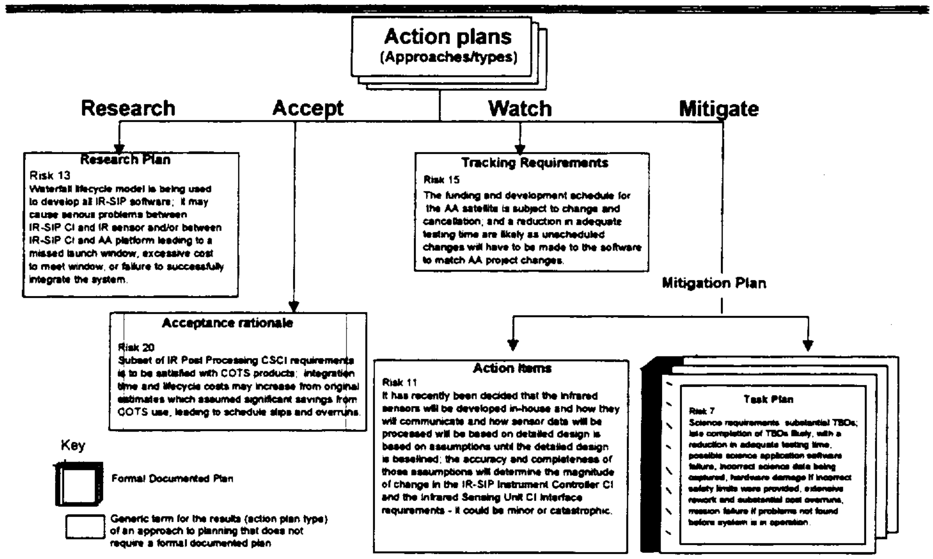
The result of planning is a documented decision about what should be done with each risk.

The decision is documented in a risk action plan.*
The types of risk action plans are:

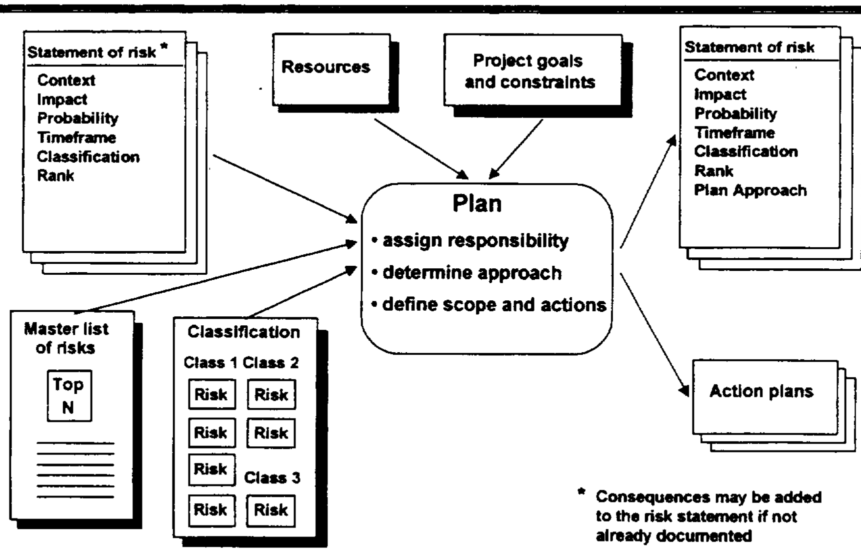
- research plan
- acceptance rationale
- tracking requirements
- mitigation plan
  - action item list
  - task plan

* The term "plan" refers to the approach for mitigating a risk and does not necessarily mean a formal documented plan.

Example - Action Plans



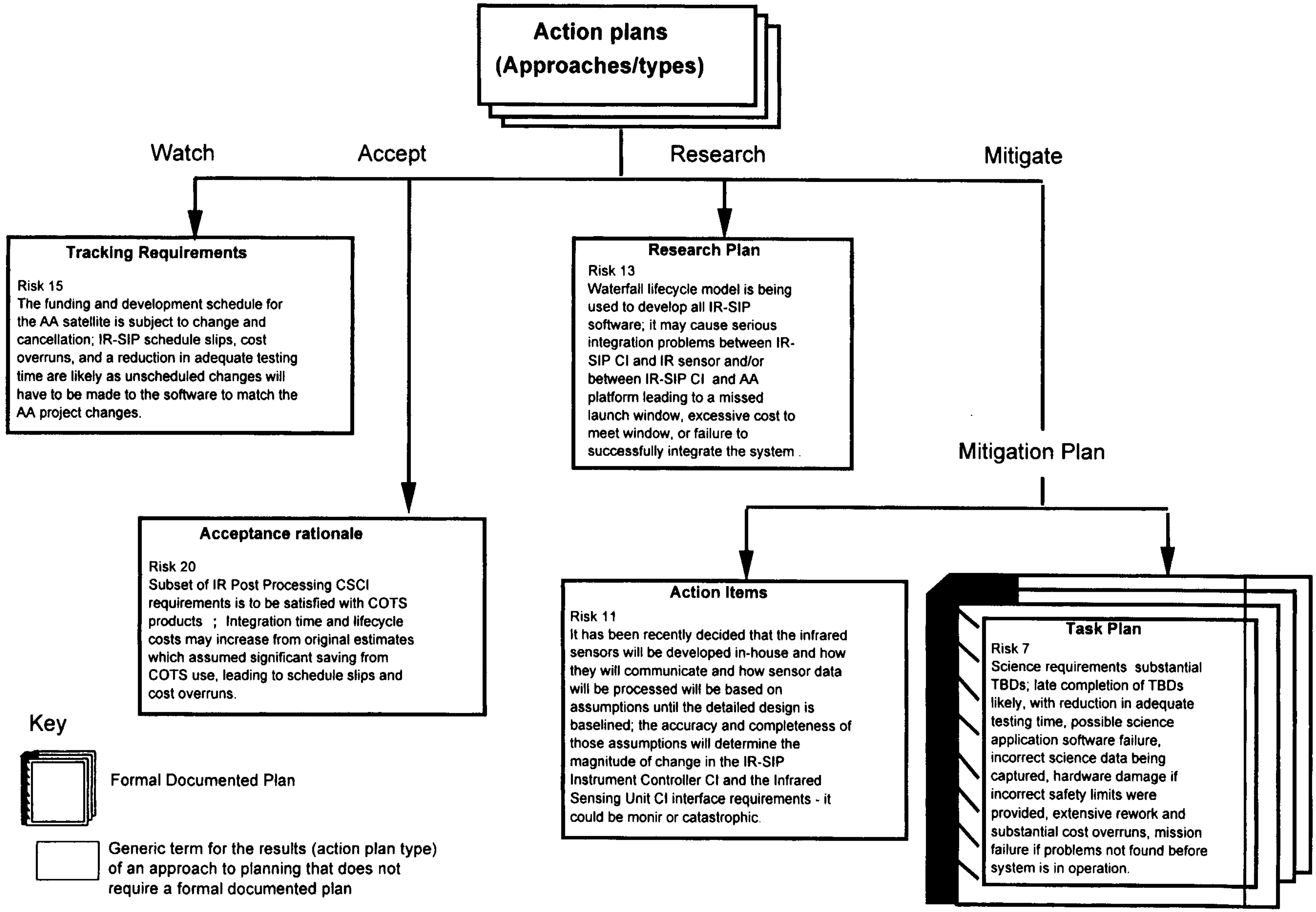
Planning Summary



* Consequences may be added to the risk statement if not already documented

Case Study

Approaches to Planning and Their Action Plans



Completed Planning Worksheet

Planning Worksheet

Risk ID 7	Responsibility J. Johnstone

Risk statement
Science requirements have substantial TBDs; late completion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.

Mitigation goals and constraints (in observable terms)
Science requirements must be completed and all related change requests submitted for implementation. No slipping of the overall development completion date is allowed. Preferable to not use overtime or additional resources but if necessary to keep completion date, do so.

Additional data (e.g., root causes, impacted elements)
Root causes - incomplete definition of reqts in early phases and inadequate scheduling to allow completion; poorly planned use of personnel (civil service and contractor); insufficient funding for contractor personnel and not enough civil servants to make up for it; science requirements not available in early phases.

Related risks
none

Alternative strategies/actions	Estimated costs
Initiate an extra contractor task to analyze, complete, research, and complete the TBD requirements	$70,000
Analyze, research, and complete TBD science requirements and submit change requests ASAP - use civil service and contractor	$10,000
Authorize contractor overtime until all requirements are complete	$105,000
Wait and see how bad it gets - slip schedule then if need to (AA satellite completion is probably going to be late as well)	worst case: $3 -8 million
Reprioritize baselined requirements and reorder builds to minimize impact of TBDs	1 person week (civil service)

Related mitigation plans
none

Strategy evaluation criteria
Minimal contractor cost, no completion date slippage

Chosen strategy/actions	Success measures
Analyze, research, and complete TBD science requirements and submit change requests ASAP - use civil service and contractor	All TBD requirements completed by July with no overtime required
Reprioritize baselined requirements and reorder builds to minimize impact of TBDs	Build order is not impacted by change requests from TBD requirements
Track progress and use contingency if necessary	Management is not surprised by failure of mitigation plan
Contingency strategy	**Contingency trigger**
Authorize contractor overtime to assist civil service. Up to 10 person weeks in contractor time allowed. Approval by Johnstone required.	Weekly status reveals that TBD requirements are not going to be documented and closed by the due dates
Drop lower level science requirements to make up for estimated development time required to complete higher priority requirements.	Insufficient time in schedule to complete all requirements (as calculated by projected impact of schedule and resource hits from change requests and current progress on implementation)

Planning Key Points - 1

- Mitigate unacceptable risks to the project.
- You can't mitigate all risks - but you need to understand which risks you are taking.
- Watch the risks you can't currently mitigate and don't want to accept.
- Unassigned risks tend to fall through the cracks.
- Don't over plan - action item lists are sufficient for most mitigation plans.

Case Study

Planning Worksheet

Planning Worksheet	
Risk ID 7	**Responsibility** J. Johnstone
Risk statement Science requirements have substantial TBDs; late completion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.	
Mitigation goals and constraints (in observable terms) Science requirements must be completed and all related change requests submitted for implementation. No slipping of the overall development completion date is allowed. Preferable to not use overtime or additional resources but if necessary to keep completion date, do so.	
Additional data (e.g., root causes, impacted elements) Root causes - incomplete definition of reqts in early phases and inadequate scheduling to allow completion; poorly planned use of personnel (civil service and contractor); insufficient funding for contractor personnel and not enough civil servants to make up for it; science requirements not available in early phases.	
Related risks none	
Alternative strategies/actions	**Estimated costs**
Initiate an extra contractor task to analyze, complete, research, and complete the TBD requirements	$70,000
Analyze, research, and complete TBD science requirements and submit change requests ASAP - use civil service and contractor	$10,000
Authorize contractor overtime until all requirements are complete	$105,000
Wait and see how bad it gets - slip schedule then if need to (AA satellite completion is probably going to be late as well)	worst case: $3 -8 million
Reprioritize baselined requirements and reorder builds to minimize impact of TBDs	1 person week (civil service)
Related mitigation plans none	
Strategy evaluation criteria Minimal contractor cost, no completion date slippage	

Chosen strategy/actions	**Success measures**
Analyze, research, and complete TBD science requirements and submit change requests ASAP - use civil service and contractor	All TBD requirements completed by July with no overtime required
Reprioritize baselined requirements and reorder builds to minimize impact of TBDs	Build order is not impacted by change requests from TBD requirements
Track progress and use contingency if necessary	Management is not surprised by failure o: mitigation plan
Contingency strategy	**Contingency trigger**
Authorize contractor overtime to assist civil service. Up to 10 person weeks in contractor time allowed. Approval by Johnstone required.	Weekly status reveals that TBD requirements are not going to be documiented and closed by the due dates
Drop lower level science requirements to make up for estimated development time required to complete higher priority requirements.	Insufficient time in schedule to complete all requirements (as calculated by projected impact of schedule and resourc hits from change requests and current progress on implementation)

Planning Key Points - 2

Communication

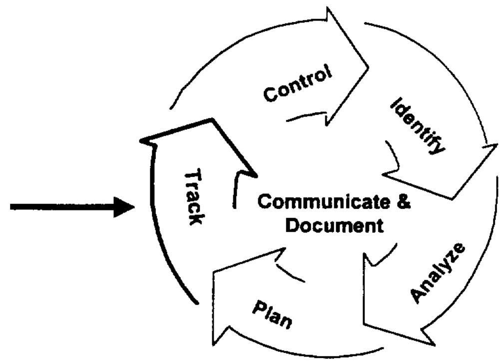
- Use teams to develop effective plans.
- Submit plans for approval and review.
- Determine tracking requirements for risks and mitigation plans

Remember project, manager, user, and customer considerations when planning:

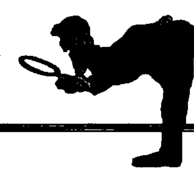
- what is currently considered important
- fixed or critical milestones
- project limits and constraints
- available resources for mitigation

Module 6

Track



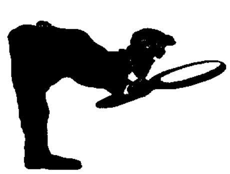
Track



Tracking

- **a process for watched and mitigated risks where related data are acquired, compiled, analyzed, and reported**

Risks can be tracked individually or in sets.

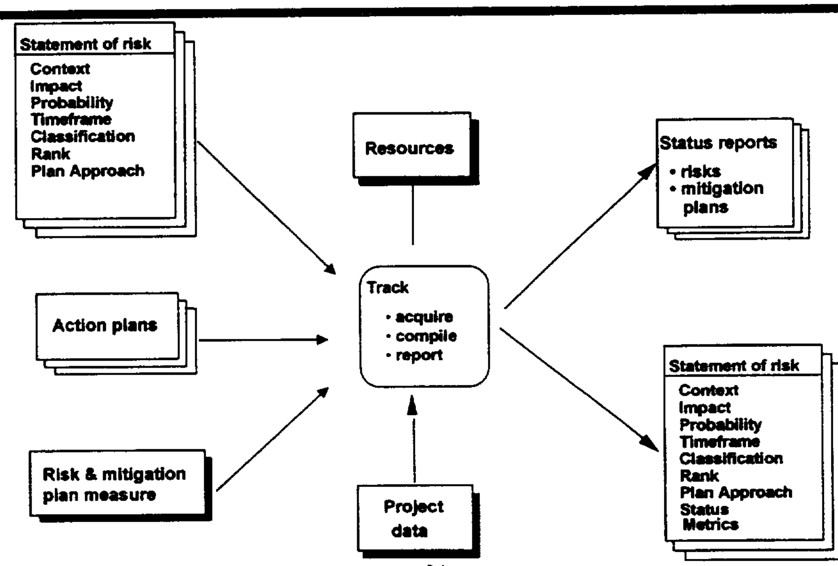


Overview

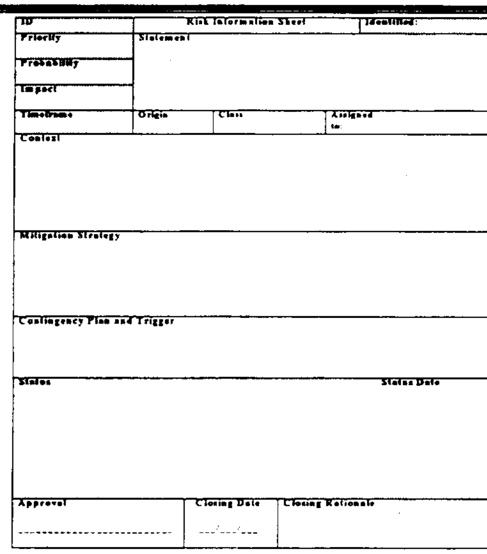
Overview of tracking activities

Tracking activities
- acquire
- compile and evaluate
- report status (plan, risk)

Track Activities Overview



Risk Information Sheet



Completed or Updated:

- **Priority**
- **Probability**
- **Impact**
- **Timeframe**
- **Status**
- **Status Date**

Tracking Risks and Plans

1. Tracking the <u>mitigation plan</u> will indicate
- **whether the plan is being executed correctly**
- **if the plan is on schedule**

2. Tracking the <u>risk attributes</u> will indicate
- **mitigation plan effectiveness**

Risk Metrics

Metrics are used to:

- measure attributes of a risk
  - impact, probability, and timeframe
  - other risk-specific attributes
- provide meaningful information to enable more informed control decisions
- assess the impact or success of a mitigation plan
- identify new risks

Acquire

Purpose:

- to collect tracking data for a given risk

Description

- a process that includes all of the steps associated with collecting information about and updating the values of risk measures and status indicators for watched and mitigated risks

Considerations When Acquiring Data

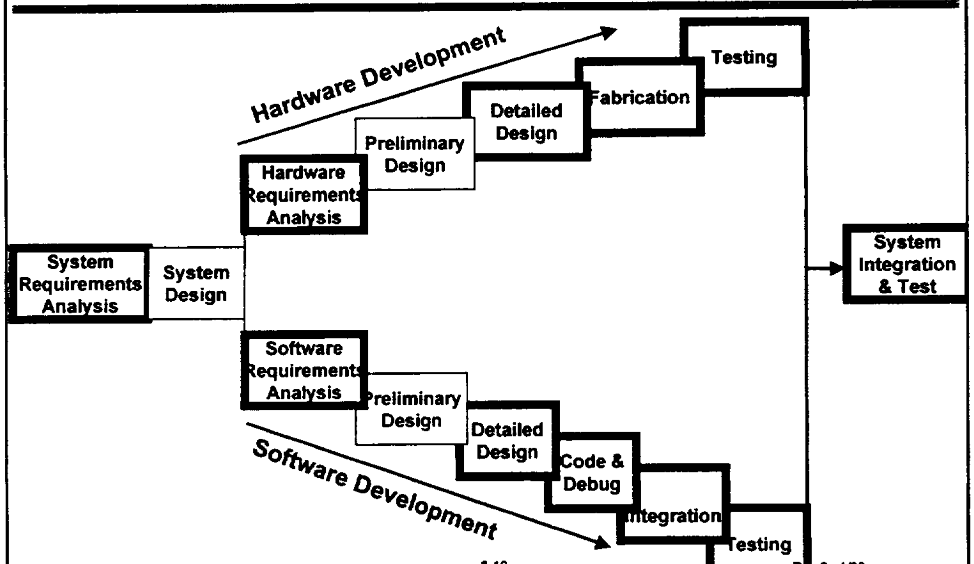
Status information is only as good as its accuracy and timeliness.

Stale data are more dangerous to decision makers than no data at all.

When a group of indicators is required, all of the data must be acquired from the same time period.

Collect the data needed to track the project's risks. Collect only what you need and use what you collect.

Metrics by Life Cycle Phases



Data Acquisition - Metrics

<u>Requirements</u>
- Ambiguity = Weak phrases
- Completeness = TBD + TBA + TBR

<u>Design & Implement</u>
- Structure/Architecture = Complexity & Size

<u>Testing</u>
- Problem report tracking = open, closed, severity
- Defect density

<u>Process</u>
- Schedule = effort, completion rates
- Budget

Compile & Evaluate

Purpose:
- organize and understand the relevant tracking data for a given risk

Description:
- a process in which data for a given risk is combined, calculated, organized, and interputed for the tracking of a risk and its associated mitigation plan

Trigger/Threshold

A value of an indicator that specifies the level at which an action, such as implementing a contingency plan, may need to be taken.

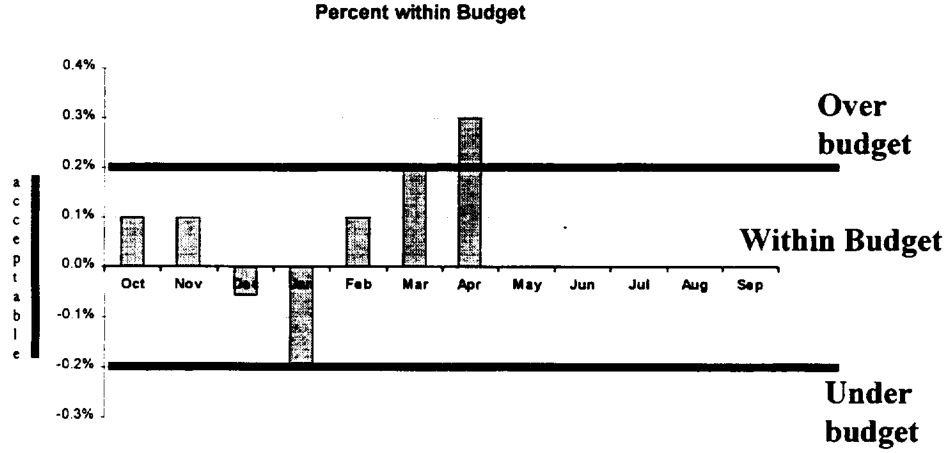
Generally used to:

- provide early warning of an impending critical event
- indicate the need to implement a contingency plan to preempt a problem
- request immediate attention for a risk

Effective if:

- does not trip unnecessarily
- is easy to calculate and report

Example - Triggers



Risk 100:Project resources (personnel number and availability) and schedules were underestimated; schedule slips, cost overruns, reduction in adequacy of development processes (especially testing time adequacy) likely.

Data Compilation & Trigger Example

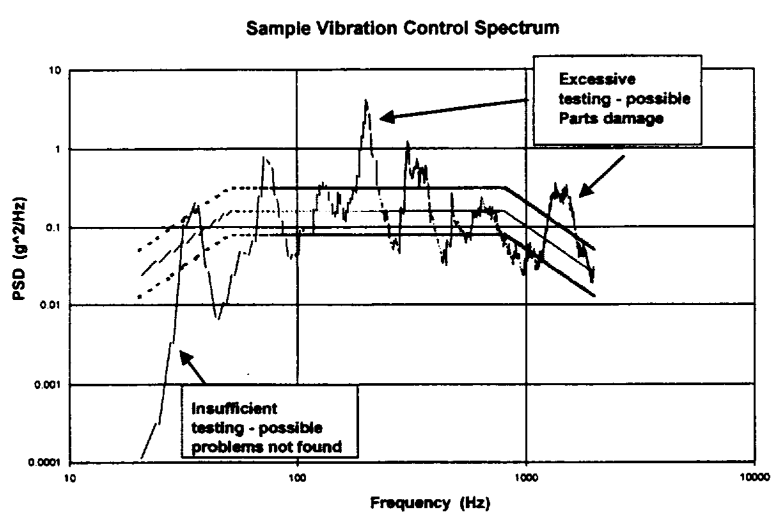
Risk # 14: Contracting a different test facility for acoustical testing; parts may be insufficiently tested or parts may be damaged with excessive testing.

Data to be collected: Vibration testing spectrum

Trigger: Upper and lower bounds dependent on component ==> excessive or insufficient testing

==> potential new risks

Data Compilation & Trigger Example



Requirements Metrics Example

Risk # 7: Science requirements have substantial TBDs; late completion, inadequate test time.

Data to be collected: terminology of document ⇒ weak phrases, incomplete terms, optional terms, TBDs, TBSs, TBAs

Trigger: >0 on any

Requirements Metrics Example - Text Analysis

56 NASA DOCUMENTS	LINES OF TEXT - Count of the physical lines of text	Imperatives - shall, must, will, should, is required to, are applicable, responsible for	Continuances - as follows, following, listed, inparticular, support	Directives - figure, table, for example, note:	Weak Phrases - adequate, as applicable, as appropriate, as a ninimum, be able to, be capable, easy, effective, not limited to, if practical	Incomplete - TBD, TBS, TBR	Options - can, may, optionally
NASA Average	4772	682	423	49	70	25	63
Level 3 Project Z	1011	588	577	10	242	1	5
Level 4 Project Z	1432	917	289	9	393	2	2

Tool available from: http://satc.gsfc.nasa.gov

Testing Metrics Example

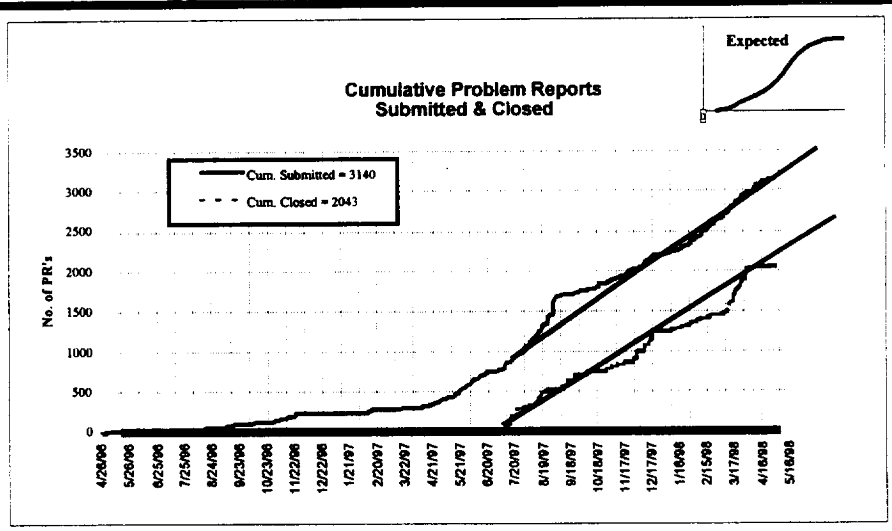
Risk # 100: Project resources and schedules were underestimated; schedule slips, cost overruns, testing time inadequate.

Data to be collected: Number open, closed, total number (Linear trend to closure)

Trigger:

- **Total number is not as expected on curve**
- **Closure rate trend will not hit 0 prior to milestone**

Testing Metrics Example - Tracking Errors/Faults/Changes



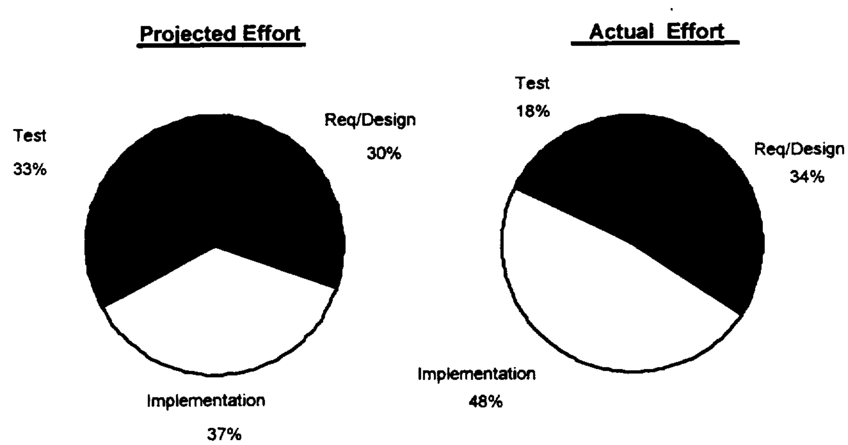
Process Metrics Example

Risk # 6: Project software schedule and resources were underestimated; schedule slips, reduction in adequate testing time.

Data to be collected : Effort per activity

Trigger: Exceeds expected percentages

Process Metrics Example - Effort per Phase



Risk - Decrease in Testing projected

Data Collection Exercise

Risk	Data to be Collected
#1 This is the first time that the software staff will use OOD; The staff may have a lower-than-expected productivity rate and schedules may slip because of the associated learning curve.	
# 20 Subset of IR Post Processing CSCI requirements is to be satisfied with COTS products; Integration time and lifecycle costs may increase from original estimates which assumed significant saving from COTS use, leading to schedule slips and cost overruns.	
#12 Resource availability estimates were overly optimistic- schedule shows all resources are available at the start of each WBS element; schedule slips, cost overruns, and reduction in adequate testing time are likely.	

Report

Purpose:
- communicate risk status reports to support effective decision making

Description:
- a process in which status information about risks and mitigation plans is communicated to decision makers and team members

Report Considerations

What information needs to be reported?

What presentation formats best present the analyzed data?

Does the information and the format of the report provide the basis needed by decision makers?

Stoplight / Fever Chart

	Condition	Risk ID	Risk Statement	Assigned To	Action Plan	Remaining Key Milestones	Comments
	Yellow	14	Contracting different test facility; insufficient testing, damage.				
	Green	7	Science reqt substantial TBDs; late completion, incomplete testing, wrong data.				
$$$	Red	6	SW schedule and resources under estimated; schedule slips, cost overruns.				

Spreadsheet Risk Tracking

Documents data in a spreadsheet format, which is periodically reviewed

Provides a concise set of risk and status information in a format that is easy to read and comprehend

Supports routine project meetings where risks are being reviewed and discussed

Example

Spreadsheet Risk Tracking

Case Study

Spreadsheet Risk Tracking

EXAMPLE

IR-SIP Monthly Project Review: Risk Status Spreadsheet – April 1, 1997

Priority	Risk ID	Risk Statement	Status Comments	Probability	Impact	Assigned To
1	22	AA Satellite Simulator is being developed; impacts to current project plan and other mitigation plans are unknown but could be significant - availability of resources to make use of simulator is questionable	New risk - resulted from closure of Risk 18.	H	H	Johnstone
2	100	Project resources (personnel number and availability) and schedules were underestimated; schedule slips, cost overruns, reduction in adequacy of development processes (especially testing time adequacy) likely.	New risk 22 has made this worse. Key personnel had designated back-ups in case availability slips, but Simulator work negates that.	H	H	Johnstone
3	23	Metrics are being reported only on a quarterly basis; schedules may slip and recognition of their slip may be too late for effective replanning to take place.	New risk identified by W. Wills	M	M	Peacock
4	7	Science requirements have substantial TBDs; late completion of TBDs likely , with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.	TBD's are being analyzed and researched. Expect completion of first set next week.	M	H	Johnstone
5	11	It has recently been decided that the Infrared sensors will be developed in-house and how they will communicate and how sensor data will be processed will be based on assumptions until the detailed design is baselined; the accuracy and completeness of those assumptions will determine the magnitude of change in the IR-SIP Instrument Controller CI and Infrared Sensing Unit CI interface requirements - it could be minor or catastrophic.	So far the assumptions we used continue to hold as we complete prototypes. Only very minor requirement changes have resulted so far and the ripple has been negligible.	L	M	Johnstone

Priority	Risk ID	Risk Statement	Status Comments	Probability	Impact	Assigne
7	13	Waterfall lifecycle model is being used to develop all IR-SIP software; it may cause serious integration problems between IR-SIP CI and IR sensor and/or between IR-SIP CI and AA platform leading to a missed launch window, excessive cost to meet window, or failure to successfully integrate the system.	Project plan revised for incremental life cycle. Recommendation to move to Watch negated by new risk 22. Revisit next month.	L	L	Everette
. . .		and other Top N risks....				
CLOSE D	2	Commercial parts suitability for space applications is unknown; parts failure may lead to system failure and use of space grade parts may cause schedule delays since space qualified parts procurement have a procurement lead time of at least 18 months.	Commercial parts appear to be working and same reliability as space qualified parts			Peacocl
CLOSE D	18	There is no AA Satellite Simulator currently scheduled for development; probable that the IR-SIP CSCI will fail when initially integrated with the actual AA Satellite since prior interface testing will not have been possible, thus software fixes will be done very late in the project schedule and may cause the launch date to slip.	Goldman authorized development of simulator on an accelerated schedule. IR-SIP's project plan must be revisited to enable us to make use of the simulator. Recommendation to close risk and open a new risk 21, accepted.			Goldma
		WATCH LIST				
W	101	Use of C++, the selected compiler, and OOD are new for software staff; decreased productivity due to unexpected learning curve may cause design and coding schedules to slip.	Training appears to be effective. only 2 people left to be trained. Calls to help desk reduced by 80%. Use of expert from ORB project has been successful. Recommend moving this risk to Watch	L	L	Everett

Priority	Risk ID	Risk Statement	Status Comments	Probability	Impact	Assigned To
W	15	The funding and development schedule for the AA satellite is subject to change and cancellation; IR-SIP schedule slips, cost overruns, and a reduction in adequate testing time are likely as unscheduled changes will have to be made to the software to match AA project changes.	No change	L	H	Johnstone
		............and all other risks which are not on the top N list and have not been accepted or closed.				

Reporting Schedule

Reports are generally delivered as part of routine project management activities:

- weekly status meetings
- monthly project meetings

The frequency of reporting depends on:

- the reporting requirements for each risk or risk set
- the manner in which the report will be used

Exception reporting may be necessary.

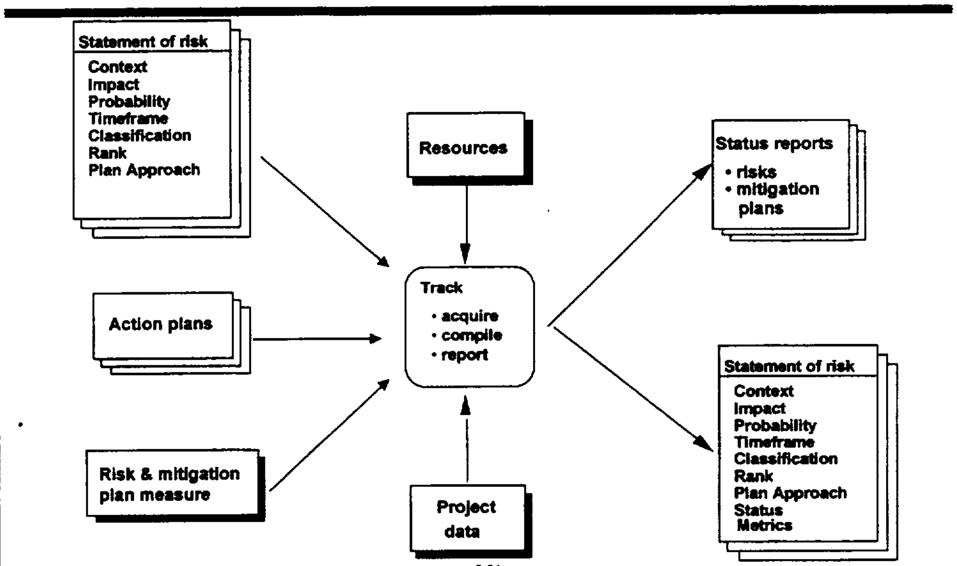
Tracking Sets of Risks

Risk sets can be tracked as an entity

If a mitigation plan has been developed for a set

- the mitigation plan status data are reported for the set
- risks in a set can also be tracked separately if the individual risks are important

Track Activities Overview

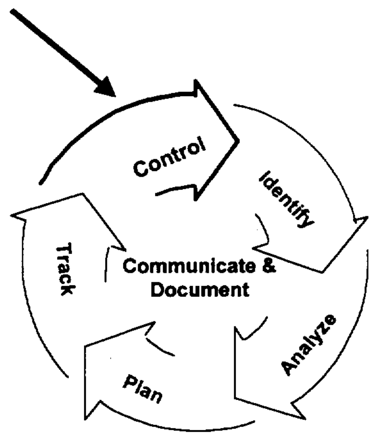


Tracking Key Points

- Tracking reports communicate information required for effective control decisions.
- Tracking information and reports can include quantitative indicator data as well as more subjective information (e.g., recommendations).
- Tracking information is not limited to formal reporting mechanisms.
- Informal reporting of risk-related information by all project personnel can aid decision making.
- Risk tracking should be integrated with standard management practices - risk management should be tailored for a project.

Module 7

Control



Control

Control
- a process in which decisions are made based on the data presented in the tracking reports

Risks can be controlled individually or in sets.

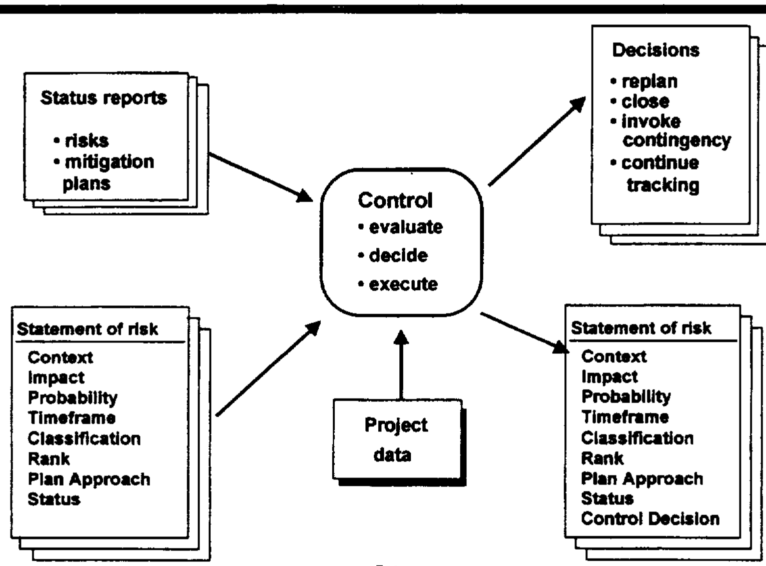
Control Overview

Control activities overview

Control activities

- evaluate tracking results
- decide risk activity
- execute

Control Activities Overview



What Is Effective Control?

Assessing the effectiveness of mitigation plans

Monitoring the quality of plan execution

Assessing significant changes in risks and trends

Determining appropriate responses

Executing the plan of attack

Communicating above information

Controlling a Set of Risks

When a set of risks is being evaluated and its trigger is reached, a decision should be made about whether to look at individual risks.

If the risk being closed is a part of a set of risks, an informed decision should be made either to close the set or to close selected risks within the set.

Risk Information Sheet

Completed Items:

- –Approval
- –Closing date
- –Closing rationale

ID	Risk Information Sheet		Identified:
Priority	Statement		
Probability			
Impact			
Timeframe	Origin	Class	Assigned to:
Context			
Mitigation Strategy			
Contingency Plan and Trigger			
Status			Status Date
Approval	Closing Date __/__/__	Closing Rationale	

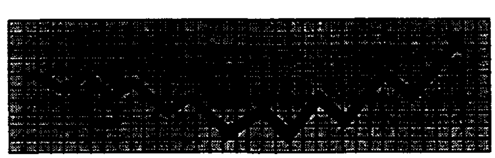
Evaluate Tracking Results

Purpose:

- allow decision makers to identify significant changes in risks, to assess the effectiveness of mitigation plans, and to accurately determine the best courses of action

Description

- uses tracking data to re-access project risks for trends, deviations, and anomalies



Metric Trend Analysis

The risk management plan can document which project metrics to track.

Trend and data analysis of project metrics can be used to identify new risks.

Trends can be observed through the evaluation of successive reports

- persistent lateness in taking action
- oscillating priority values
- significant changes in the number of high impact risks or risks of a particular type

Testing Metrics - Example #1 Tracking Errors/Faults/Changes

Given concerns about inadequate Test Resources and Schedules, e.g.,

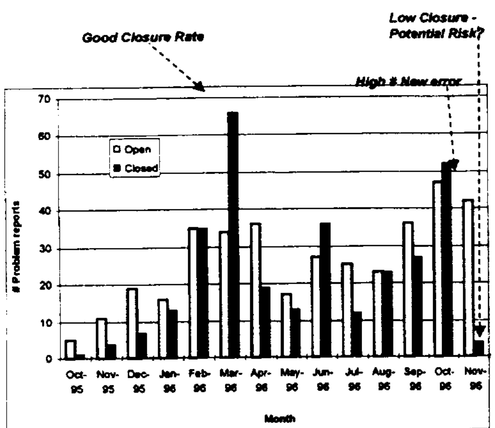
#6 - Project software schedule and resources were underestimated; Schedule slips, cost overruns, and a reduction in adequate testing time are likely results.

#21 - Poor communication between the AA Project's system engineering team and the IR-SIP instrument team; substantial errors may occur in the interface between the IR instrument and the AA satellite and spacecraft integration testing may take longer than planned and consume more resources for software changes to correct the problems.

What approach would you take? What would you collect? What trends would you expect to see evolve? etc.

Testing Metrics - Sample Solution #1
Tracking Errors/Faults/Changes

Open/Closed



Testing Ends in 3 Months (Feb '97)

Error Counts

Code Module	Count	Percent Of Total
ES1CHECK	15	9.1%
EPHEX	6	3.7%
EEEQP	5	3.0%
TRPAR	5	3.0%
ACTHR	4	2.4%
CANAC	4	2.4%
CSAPM	4	2.4%
CSSRD	4	2.4%
MAMUS	4	2.4%
PRADS	4	2.4%
UCVMP	4	2.4%

(Top 1/3 of all Errors Found)

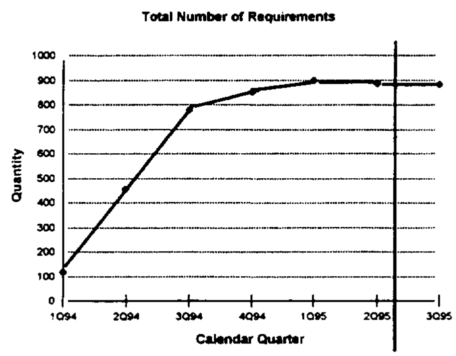
Trending Metrics - Example #2

Given concerns about Unstable or Incomplete requirements, which metrics might be useful in controlling this risk area?

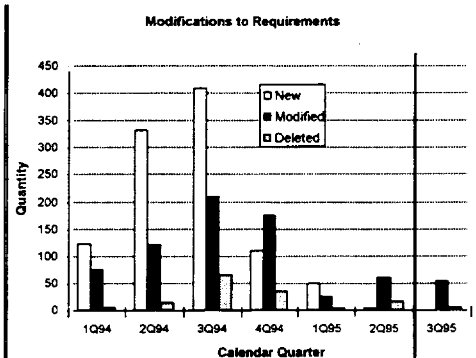
#7 - Science requirements have substantial TBDs; late completion of TBDs likely, with reduction in adequate testing time, possible science application software failure, incorrect science data being captured, hardware damage if incorrect safety limits were provided, extensive rework and substantial cost overruns, mission failure if problems not found before system is in operation.

What would you collect? What trends would you expect to see evolve? etc.

Requirements Metrics -Sample Solution #2
Completeness & Volatility Analysis



CRR
Looks Good!
(Stable)



CRR
Excessive Changes!
NOT Stable

Combination of BOTH views indicates risk area - requirements are NOT YET stable

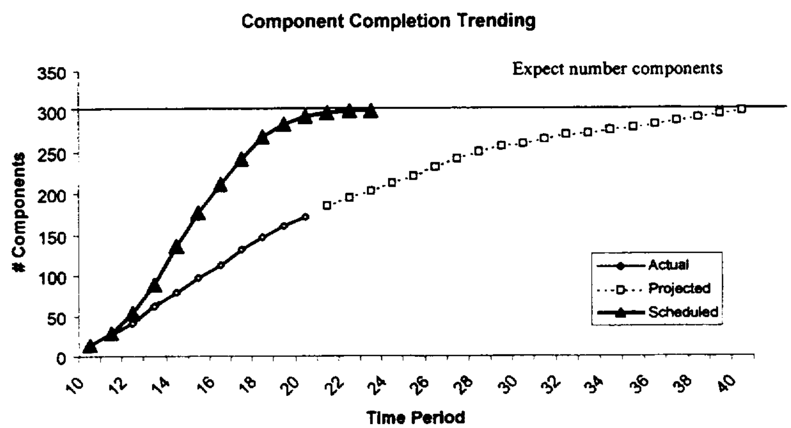
Trending Metrics - Example #3

Recall concerns about inadequate Test Resources and Schedules.

#6 - Project software schedule and resources were underestimated; Schedule slips, cost overruns, and a reduction in adequate testing time are likely results.

Another approach to the same risk - completion rates

Trend Analysis -Sample Solution #3
Completion Metrics



Decide

Purpose:
- **ensure that project risks continue to be managed effectively**

Description:
- **uses tracking data to determine how to proceed with project risks**
  - **close**
  - **continue tracking and executing the current plan**
  - **replan**
  - **invoke a contingency plan**

Action #1 - Close a Risk

A closed risk is one that no longer exists or is no longer cost effective to track as a risk.

This occurs when:
- Probability falls below a defined threshold
- Impact lies below a defined threshold
- the risk has become a problem and is tracked

Closure:
- recommended by person responsible for the risk

The closure is reported, database is updated and the originator is advised

Action #2 - Continue Tracking and Executing Current Plan

No additional action is taken when:

- analysis of the tracking data indicates that all is going as expected
- project personnel decide to continue tracking the risk or mitigation plan as before

Action #3 - Replan

A new or modified plan is required when

- the threshold value has been exceeded
- indicators show that the action plan is not working
- an unexpected adverse trend is discovered

This equates to Mid-Course Correction

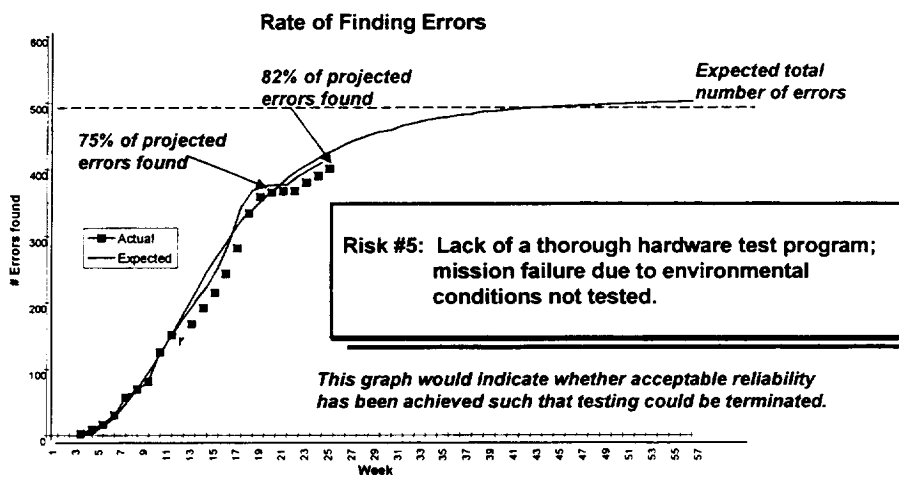
Action #4 - Invoke a Contingency Plan

A contingency plan is invoked when:

- a trigger has been exceeded
- some other related action needs to be taken

The risk and its mitigation plan continue to be tracked after the contingency plan has been executed.

Example - Continual Data Tracking and Analysis (Risk #5)



Risk #5: Lack of a thorough hardware test program; mission failure due to environmental conditions not tested.

Risk is dependent on scheduled end of testing

Execute

Purpose:

- implement both the decision made about a risk and mitigation plan as well as to ensure that all decisions are appropriately *documented for future* reference and historical record maintenance
- ensure approval and resources are allocated

Description:

- the process where control decisions are implemented

Mitigation Status Report

Provides a way to track mitigation plans on a periodic basis.

Provides concise and visual summaries of project risks.

Summarizes risk data and the status of mitigation efforts for management.

Mitigation Status Report Format

A mitigation status report can include:

- Textual information
  - Risk information
  - Risk status
  - Root causes and mitigation actions
  - Other information chosen by project
- Graphical information:
  - Time graph tracking risk indicators
  - Gantt chart or PERT chart tracking the plan
  - Stoplight chart tracking plan status
  - Other information chosen by project

Example

Mitigation Status Report

Mitigation Status Report

Requirements

Risk ID: 7

Science requirements likely to change substantially; reduction in testing time leading to possible application software failure and extensive rework and substantial cost overruns are likely.

Date: 5/24/96

Approach: [ ] Watch [ ] Accept [X] Mitigate

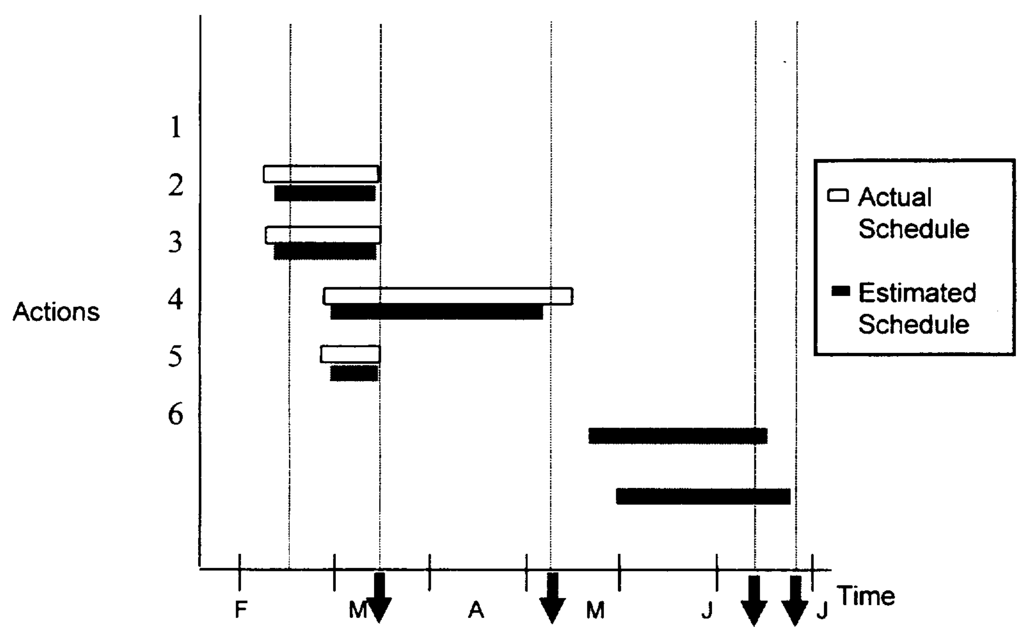
Risk Status:

Impact (I)	H
Probability	M
Current Risk Exposure (RE)	H
Initial Risk Exposure (RE)	H

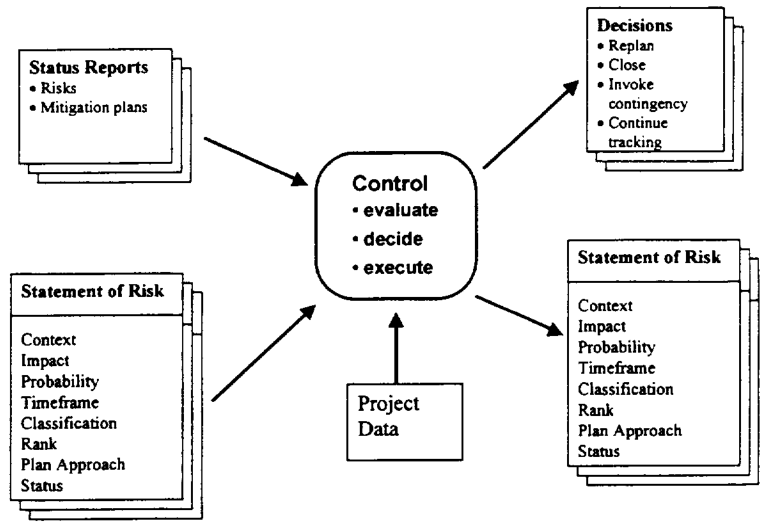
[ ] Green [X] Yellow [ ] Red

Root Causes:

Description	Mitigation Summary	Actions
Inadequate scheduling to allow for requirements definition.	Reprioritize baselined requirements and estimate impact to schedule.	1, 2
All of the science requirements are still not available.	Complete TBD requirements.	3, 4, 5, 6



Control Summary



Risk Information Sheet after Tracking and Control

ID	11	Risk Information Sheet	Identified: 11/ 1/ 95
Priority	7	Statement It has recently been decided that the Infrared sensors will be developed in-house and how they will communicate and how sensor data will be processed will be based on assumptions until the detailed design is baselined; the accuracy and completeness of those assumptions will determine the magnitude of change in the IR-SIP Instrument Controller CI and Infrared Sensing Unit CI interface requirements - it could be minor or catastrophic.	
Probability	M		
Impact	M		

Timeframe	N	Origin K. Green	Class Requirements	Assigned to: J. Johnstone

Context The AA program is in the Systems Preliminary Design Phase and the IR-SIP project software is in the Software Specification Phase.

- This is the first time these sensors will be used on a NASA mission. They will still be under design and definition during the IR-SIP Controller's software specification through implementation phases. Therefore, assumptions about the interface will have to be made in implementing the IR-SIP CSCI and if those assumptions are incorrect, then software rewrites will be necessary. We do have access to a reasonable set of assumptions and information from a contractor who has developed very similar sensors, but again, we don't really feel 100% confident in those assumptions.
- Problems were not anticipated in the current success-oriented schedule so there is no slack time if the impact of the changes is major. Schedule slips, cost overruns, and reduction in adequate testing time are all possible if the assumptions prove false.
- System testing does not begin until very late in the development, so if problems are encountered there is usually no time to make changes in the hardware. Therefore, software must provide work-arounds for problems encountered.

Mitigation Strategy

[Mitigation goal/success measures: Reduce the probability and impact of incorrect interface assumptions to a minimum: estimated low probability and low impact. Ideally, completion of prototype tests will show that assumptions we got from EasySensor were correct and there is no impact at all.]

1. Build prototypes of the IR-SIP CSCI software primitives needed to control the interface with the Infrared Sensing Unit early in the software requirements phase.
   - Start by 1/10/96. Prototype should contain all the functionality defined by that date for the configuration of the Infrared Sensing Unit. Complete by 1/30/96.
2. Have early interface tests with the Infrared Sensor Unit to confirm functionality and control issues. Allocate enough time for software work-arounds to be developed if problems arise.

Mitigation Strategy (cont.)

- Test of the interface between the two subsystems will be completed by 2/3/96.
- Second prototype to command the transmission of sensor data from the Unit to the

Contingency Plan and Trigger

Trigger: If the 2/12/96 or 2/28/96 dates cannot be met, put the contingency plan in place

Contingency Plan: Elevate this as one of the top 10 project risks and request that project reserves be used to pay for additional contract support to get the two sets of requirements firmed up (i.e., configuration and data transfer). If additional contract resources are not available, slip the schedule for completion of the prototypes to be done by March 20, and request that project reserves be used to pay for additional resources to be added to the software design and implementation to make up the schedule slip.

Status	Status Date
Interface tests in progress - no significant difficulties found so far. Expected completion of tests on 2/26	2/20/96
Second prototype complete	2/7/96
Testing of the interface complete, ran a bit late but no significant difficulties found with the interface	2/4/96
First prototype complete	2/1/96

Approval	Closing Date	Closing Rationale
______________	_/_/_	

Case Study

Risk Information Sheet After Tracking and Control

<table>
<tr><td>ID 11</td><td colspan="3">Risk Information Sheet</td><td>Identified:
11/ 1/ 95</td></tr>
<tr><td rowspan="2">Priority 7
Probability M
Impact M
Timeframe N</td><td colspan="4">Statement
It has recently been decided that the Infrared sensors will be developed in-house and how they will communicate and how sensor data will be processed will be based on assumptions until the detailed design is baselined; the accuracy and completeness of those assumptions will determine the magnitude of change in the IR-SIP Instrument Controller CI and Infrared Sensing Unit CI interface requirements - it could be minor or catastrophic.</td></tr>
<tr><td>Origin
K. Green</td><td>Class
Requirements</td><td colspan="2">Assigned to: J. Johnstone</td></tr>
</table>

Context The AA program is in the Systems Preliminary Design Phase and the IR-SIP project software is in the Software Specification Phase.

- This is the first time these sensors will be used on a NASA mission. They will still be under design and definition during the IR-SIP Controller's software specification through implementation phases. Therefore, assumptions about the interface will have to be made in implementing the IR-SIP CSCI and if those assumptions are incorrect, then software rewrites will be necessary. We do have access to a reasonable set of assumptions and information from a contractor who has developed very similar sensors, but again, we don't really feel 100% confident in those assumptions.
- Problems were not anticipated in the current success-oriented schedule so there is no slack time if the impact of the changes is major. Schedule slips, cost overruns, and reduction in adequate testing time are all possible if the assumptions prove false.
- System testing does not begin until very late in the development, so if problems are encountered there is usually no time to make changes in the hardware. Therefore, software must provide work-arounds for problems encountered.

Mitigation Strategy

[**Mitigation goal/success measures:** Reduce the probability and impact of incorrect interface assumptions to a minimum: estimated low probability and low impact. Ideally, completion of prototype tests will show that assumptions we got from EasySensor were correct and there is no impact at all.]

1. Build prototypes of the IR-SIP CSCI software primitives needed to control the interface with the Infrared Sensing Unit early in the software requirements phase.
    - Start by 1/10/96. Prototype should contain all the functionality defined by that date for the configuration of the Infrared Sensing Unit. Complete by 1/30/96.
2. Have early interface tests with the Infrared Sensor Unit to confirm functionality and control issues. Allocate enough time for software work-arounds to be developed if

problems arise.

Mitigation Strategy (cont.)

- Test of the interface between the two subsystems will be completed by 2/3/96.
- Second prototype to command the transmission of sensor data from the Unit to the IR-SIP CSCI will be started by 2/12/96 and completed by 2/20/96.
- All subsequent interface tests will be performed by 2/28/96.

3. Feed information from the two prototype tests into updates to the Interface Requirements Specification and the associated sections of the schedule by 3/2/96.
4. Determine the impact of the revised requirements by 3/6/96.

Contingency Plan and Trigger

Trigger: If the 2/12/96 or 2/28/96 dates cannot be met, put the contingency plan in place.

Contingency Plan: Elevate this as one of the top 10 project risks and request that project reserves be used to pay for additional contract support to get the two sets of requirements firmed up (i.e., configuration and data transfer). If additional contract resources are not available, slip the schedule for completion of the prototypes to be done by March 20, and request that project reserves be used to pay for additional resources to be added to the software design and implementation to make up the schedule slip.

Status	Status Date
Interface tests in progress - no significant difficulties found so far. Expected completion of tests on 2/26	2/20/96
Second prototype complete	2/7/96
Testing of the interface complete, ran a bit late but no significant difficulties found with the interface	2/4/96
First prototype complete	2/1/96

Approval	Closing Date	Closing Rationale
________	__/__/__	

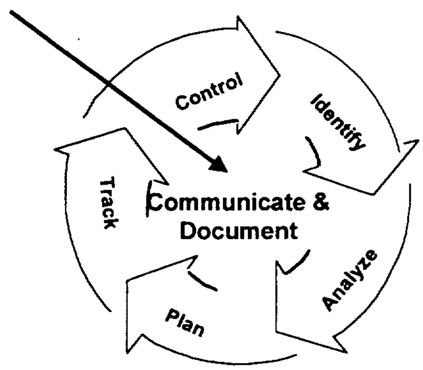
Control Key Points

- Control Decisions are based on current information as well as experience and are required to respond to changing conditions in watched and mitigated risks.

- Risk tracking and control should be integrated with standard project management practices - risk management should be tailored for a project.

Module 8

Communicate & Document



Overview

What is communication?

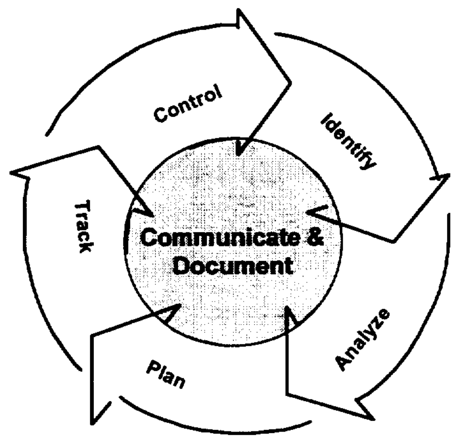
Relationship to other paradigm functions

Enablers to communication

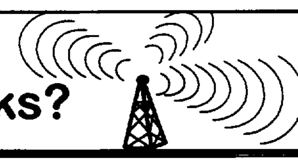
Barriers to communication

Types of Documentation

Relationship To Other Paradigm Functions



Why Communicate Risks?



Makes risks, plans, actions, concerns, exchanges, forecasts, and progress known

Ensures the visibility of risk information

To enable all project members to participate in defining and managing risks

Ensures understanding of risks and mitigation plans

Establishes an effective, on-going dialog between the manager and the project team

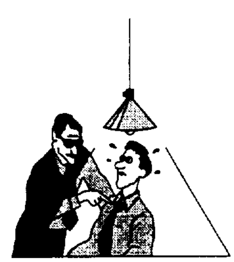
Ensures appropriate attention is focused on issues and concerns

Enablers to Communication

- Defining clear project roles and responsibilities
- Making risk actions and decisions visible
- Being a role model
- Establishing an internal champion
- Rewarding positive behavior

Barriers to Communication

- Ready-fire-aim
- Don't tell me your problem
- Shoot the messenger
- Liar's poker
- Mistrust
- Value differences
- Hidden agendas
- Differential knowledge
- Placing blame
- Inactive listening



Types of Documentation

Risk Management Plan
Risk Implementation Plan
Risk Information Sheets
Risk Analysis Reports
Risk Mitigation Status Reports

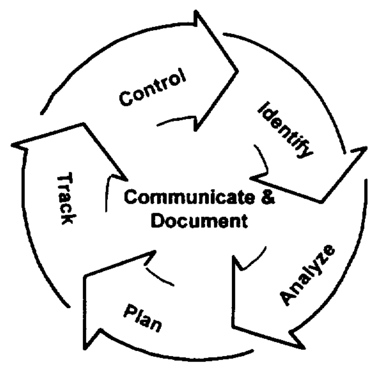
Risk Database
Tracking Logs
Test Reports

Communicate & Document Key Points

- People must feel empowered to share their issues and concerns with each other in an open manner, both formally and informally.
- Open communication creates a better understanding of the status and progress of the project because it brings forth perspectives of everyone on the project.
- Management needs to create a culture that eliminates communication barriers and develops communication enablers.
- All documentation is useful as a communication tool.

Module 9

How To Implement Continuous Risk Management



Overview - How to implement CRM

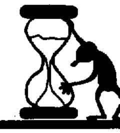
Frequently Asked Questions:

- When do I start?
- Who's involved?
- What do I need?
- What should I choose?
- What actions should I take?

Hints and Tips

Things to Watch Out For

When do I Start CRM?



Opportunity	*Actions*
Pre-contract activity	Include risk management provisions in the solicitation and statement of work.
Major project milestones (e.g., contract award)	Prepare for a major project decision point, and the need to increase knowledge about risks for improved strategic planning.
Major project review	Prepare for standard reviews, such as design reviews, functional tests.

Best time to start is at the beginning. Risk information can help in planning and budgeting.

Who's Involved? - 1

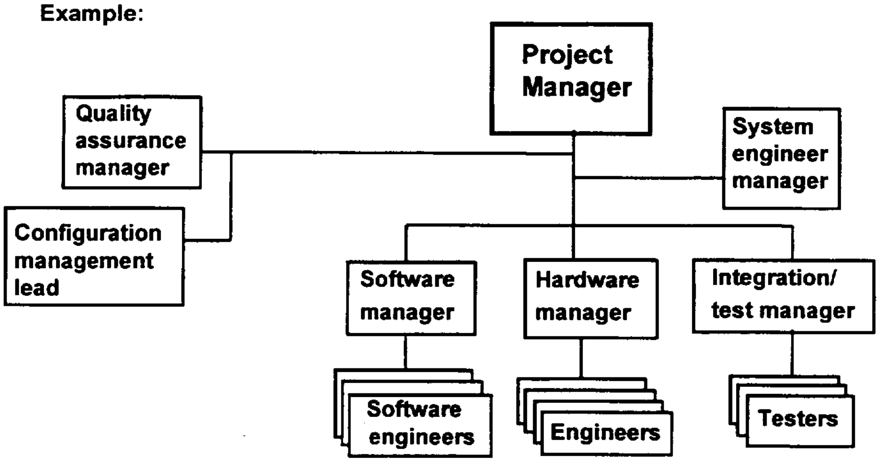
Role/Description	*Responsibilities and Tasks*
Sponsor (e.g., senior mgr., VP, division chief)	• Provide visible support and encouragement • Reward effective management of risks
Project manager (responsible for ultimate success of project)	• Provide resources and funding • Reward effective management of risks • Monitor progress
Champion (advocates new technology or process within the project)	• Publicize and promote CRM • Coordinate changes and improvements on the project
Change agents (plan and implement changes in organizations and projects	• Assist with recommendations of plans • Evaluate existing and new tools

Who's Involved? - 2

Role/Description	*Responsibilities and Tasks*
Facilitators (trained in meeting skills, conflict resolution, tools, etc., - act individually or as a team)	• Conduct training sessions • Provide CRM expertise • Provide consulting during evaluation of progress
Technical managers (e.g., team or functional leads, such as software/hardware manager, test mgr., etc.)	• Encourage and support use of CRM within their teams • Report risk information to project manager • Evaluate progress within their teams
Project personnel (e.g., software or hardware engineers, testers, etc.)	• Add CRM activities to day-to-day operations • Maintain open communication about risks

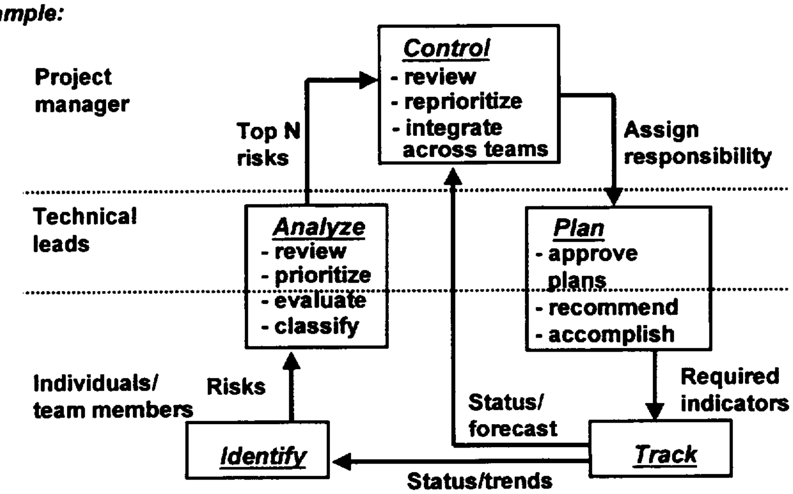
You need an . . . Organization Structure

Example:



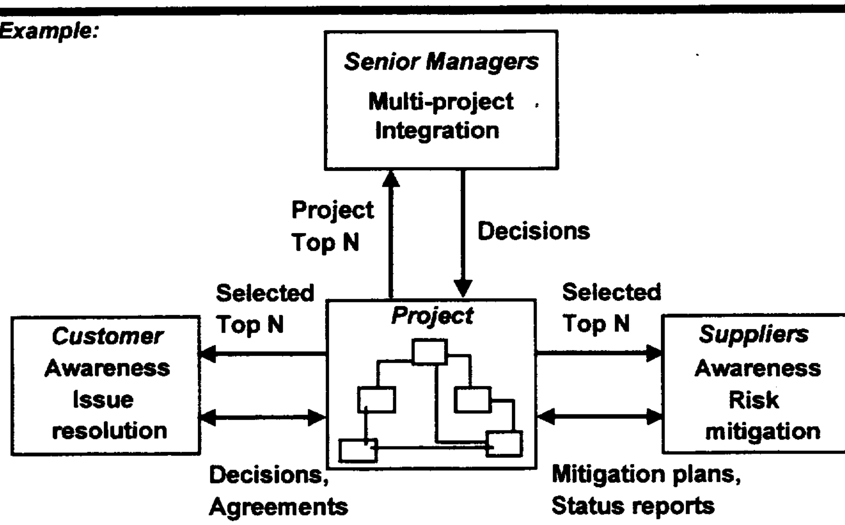
You need . . .
Internal Communication

Example:



You need . . .
External Communication

Example:



You need . . .
Assigned Roles & Responsibilities

Example:

IR-SIP Personnel

Who	Responsibilities
Individuals	Software engineers, testers, leads, and project manager • identify new risks • estimate probability, impact, and timeframe • classify risks • recommend approach and actions • track risks and mitigation plans (acquire, compile, and report)
S/W CSCI, CM, and Test Managers	Software engineering leads for each CSCI • ensure accuracy of probability/impact/timeframe estimates and the classification • review recommendations on approach and actions • build action plans (determine approach, define scope & actions) • report their top N risks and issues to the project manager • collect and report general risk management measures/metrics
Software Project Manager, Hardware Project Manager, etc.	• integrates risk information from all technical leads • reprioritizes all risks to determine top N risks in each area (software, hardware, etc.) • makes control decisions (analyze, decide, execute) for risks (e.g., Software Project Manager controls software risks) • authorizes expenditure of resources for mitigation • assigns or changes responsibility for risks and mitigation plans within the CSCI, CM, and test areas • handles communication IR-SIP project manager
IR-SIP Project Manager; IR-SIP Project Systems Engineer	• integrates risk information from all software, hardware, and CM leads • reprioritizes all risks to determine top N project risks • makes control decisions (analyze, decide, execute) for Top N project risks • authorizes expenditure of project resources for mitigation • assigns or changes responsibility for risks and mitigation plans within the project (e.g., moving responsibility for a risk from software to hardware) • handles communication with AA program manager • reviews general risk management measures/metrics with Quality Assurance during each quarter to evaluate effectiveness of risk management

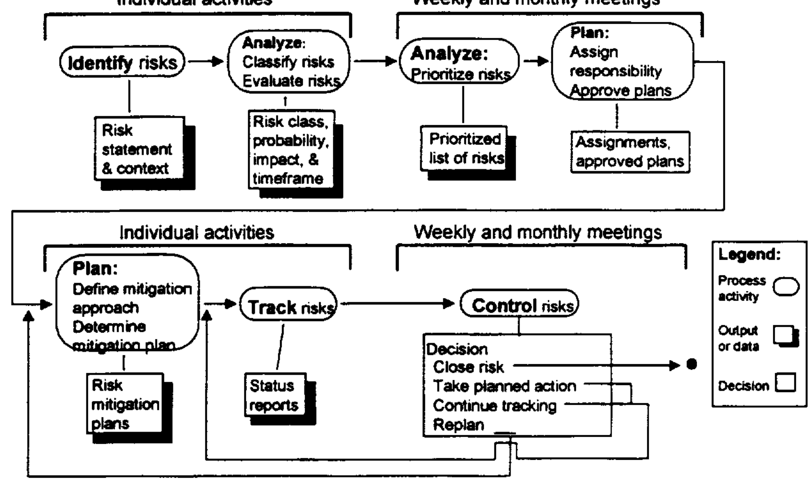
You need . . .
Established Meetings

Weekly Team Meetings
- establish priority of team's risks
- assign responsibility for new risks
- review and approve mitigation plans

Monthly Project Meetings
- Leads present the team's Top N risks (and mitigation plans)
- Project manager Leads decide on appropriate action
- Project manager determines allocation of resources for mitigation discretionary funds for technical leads

You need . . .
Process and Data Flow

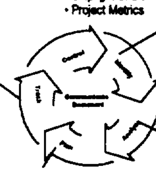
Example:



You must choose your . . .
Methods and Tools

Risk Management Plan

A Risk Management Plan documents how risks will be managed on a project: the process, activities, milestones, and responsibilities associated with risk management. It is a subset of the project plan and is written before the project begins.



Control
- Cause and Effect Analysis
- Closing a Risk
- Cost-Benefit Analysis
- List Reduction
- Mitigation Status Report
- Multivoting
- PERT Chart
- Problem-Solving Planning
- Risk Information Sheet
- Spreadsheet Risk Tracking
- Stoplight Chart
- Project Metrics

Identify
- Baseline Identification and Analysis
- Brainstorming
- Periodic Risk Reporting
- Project Profile Questions
- Risk Information Sheet
- Short TBQ
- Taxonomy-Based Questionnaire (TBQ)
- TBQ Interviews
- Voluntary Reporting
- Project Metrics
- FMEA
- FTA

Track
- Bar Graph
- Mitigation Status Report
- Risk Information Sheet
- Spreadsheet Risk Tracking
- Stoplight Chart
- Time Correlation Chart
- Time Graph
- Project Metrics
- SPC

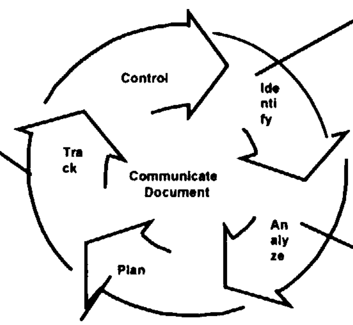
Analyze
- Affinity Grouping
- Baseline Identification and Analysis
- Binary Attribute Evaluation
- Comparison Risk Ranking
- Multivoting
- Pareto Top N
- Potential Top N
- Taxonomy Classification
- Risk Information Sheet
- Top 5
- Tri-level Attribute Evaluation
- FMEA
- FTA

Plan
- Action Item List
- Baseline Planning
- Planning Decision Flowchart
- Planning Worksheet
- Problem-Solving Planning
  - Affinity Grouping
  - Brainstorming
  - Cause and Effect Analysis
  - Cost-Benefit Analysis
  - Gantt Charts
  - Goal-Question-Measure
  - Interrelationship Digraph
  - List Reduction
  - Multivoting
  - PERT Chart
  - Work Breakdown Structure
- Risk Information Sheet
- WCA

Methods and Tools

Risk Management Plan

A Risk Management Plan documents how risks will be managed on a project: the process, activities, milestones, and responsibilities associated with risk management. It is a subset of the project plan and is written before the project begins.



Control

- Cause and Effect Analysis
- Closing a Risk
- Cost-Benefit Analysis
- List Reduction
- Mitigation Status Report
- Multivoting
- PERT Chart
- Problem-Solving Planning
- Risk Information Sheet
- Spreadsheet Risk Tracking
- Stoplight Chart
- Project Metrics

Identify

- Baseline Identification and Analysis
- Brainstorming
- Periodic Risk Reporting
- Project Profile Questions
- Risk Information Sheet
- Short TBQ
- Taxonomy-Based Questionnaire (TBQ)
- TBQ Interviews
- Voluntary Reporting
- Project Metrics
- FMEA
- FTA

Track

- Bar Graph
- Mitigation Status Report
- Risk Information Sheet
- Spreadsheet Risk Tracking
- Stoplight Chart
- Time Correlation Chart
- Time Graph
- Project Metrics
- SPC

Plan

- Action Item List
- Baseline Planning
- Planning Decision Flowchart
- Planning Worksheet
- Problem-Solving Planning
  - Affinity Grouping
  - Brainstorming
  - Cause and Effect Analysis
  - Cost-Benefit Analysis
  - Gantt Charts
  - Goal-Question-Measure
  - Interrelationship Digraph
  - List Reduction
  - Multivoting
  - PERT Chart
  - Work Breakdown Structure
- Risk Information Sheet
- WCA

Analyze

- Affinity Grouping
- Baseline Identification and Analysis
- Binary Attribute Evaluation
- Comparison Risk Ranking
- Multivoting
- Pareto Top N
- Potential Top N
- Taxonomy Classification
- Risk Information Sheet
- Top 5
- Tri-level Attribute Evaluation
- FMEA
- FTA

You should carefully . . .
Adapt to Your Project

Purpose:
- make maximum use of existing, effective project management processes and methods while integrating a set of proactive risk management activities
- document the tailored processes, methods, and tools in a risk management plan
- define a schedule for transitioning specific methods, tools, and activities into the project

Description:
- tailors risk management processes, methods, and tools for use on the project

You must choose your . . .
Risk Database

- A database is the simplest means of retaining and keeping risk information up to date.
- Data entry forms and reports can be used as the risk information sheet, spreadsheet, and other templates.
- A risk database enables documentation of lessons learned, trend analysis, pattern analysis to support identifying common risks (and solutions) across projects.

One Choice -
NASA Software Risk Management Database

- Developed at NASA Lewis to help capture & track project risks
- Based on experience and the SEI *Continuous Risk Management Guidebook*
- Contains most of the items found on the SEI "Risk Information Sheet"
- Further information available from:

  http://www-osma.lerc.nasa.gov/srmd/risk0.htm
- Database can be downloaded from the net if you have Access 7.0 or greater

First -
Document Your Plan

Risk Management Plan:

- Overview of Risk Management process
- Project Organization & Responsibilities
- Risk Management activities in detail
- Budget, resources & milestones for risk management activities and risk mitigation
- Procedure for documenting risks

Exercise - Sample Risk Management Plan

IR-SIP's Risk Management Plan can serve as DID, with example text, for your project to use.

Take 10 Minutes to read the IR-SIP risk Management Plan, then we will walk through it.

Second - Document Implementation

Risk Implementation Plan:

- **Sponsorship**
- **Project Organization & Responsibilities for transition**
- **Risk Management activities in detail**
- **Budget, resources & milestones for transition effort**
- **Evaluation measures and completion criteria**
- **Transition risks and mitigation plans**
- **Establish baseline method**

Case Study

IR-SIP Risk Management Plan Outline

Baselined:
Last Modified:
Owner:
Purpose:

Section 1. Introduction
- *1.1 Purpose and Scope*
- *1.2 Assumptions, Constraints, and Policies*
- *1.3 Related Documents and Standards*

Section 2. Overview of Risk Management Practice
- *2.1 Overview*
- *2.2 Process and Data Flows*
- *2.3 Project Management Integration (optional)*

Section 3. Organization
- *3.1 Organizational Chart*
- *3.2 Project Communication and Responsibilities*
- *3.2 AA Program Responsibilities*
- *3.3 Contractor Responsibilities*

Section 4. Practice Details
- *4.1 Establishing Baselines and Reestablishing Baselines*
- *4.2 Identifying Risks*
- *4.3 Analyzing Risks*
- *4.4 Planning Risks*
- *4.5 Tracking and Control of Risks*
- *4.6 Summary of Methods and Tools*

Section 5. Resources and Schedule of Risk Management Milestones

Section 6. Documentation of Risk Information

Case Study

IR-SIP Risk Management Plan

Baselined: 11/15/95

Last Modified: N/A

Owner: J. Johnstone/IR-SIP Project Manager

Purpose: This plan documents the practice of risk management as tailored to the IR-SIP Project. This plan will be updated on 2/25/96 and 4/25/96 to reflect changes and improvements to the risk management practice based on the evaluation results.

Section 1. Introduction

This plan will direct the processes, methods, and tools used to manage risks in the IR-SIP Project. All project personnel are responsible for following this plan. This plan is part of the IR-SIP Project Management Plan suite of documents.

1.1 Purpose and Scope

This plan will define the practice of risk management as it should be performed once it reaches maturity within the IR-SIP Project. This document does not address risk management within the AA Program.

1.2 Assumptions, Constraints, and Policies

This plan does not address the process of putting a new risk management practice in place (in other words, the actual transition process - that is documented in the Implementation Plan). This plan defines the risk management practice for the IR-SIP Project. It is recognized that this plan addresses a new practice being put into place on a project that is already in progress and that this plan is the first of its kind for IR-SIP. It is expected that significant changes and improvements will be necessary over the course of time as risk management is adopted by IR-SIP. Therefore, any corrections should be forwarded to the plan owner. Change recommendations should be submitted on the Change Documentation Request Form 1246.

1.3 Related Documents and Standards

IR-SIP Risk Management Implementation Plan will guide the technology transition process. It directs the flow of activities associated with getting the risk management practice defined in *this* plan established and ongoing.

IR-SIP Project Management Plan directs the activities of the overall project. The Risk Management Plan is subordinate to project management plan.

Section 2. Overview of Risk Management Practice

2.1 Overview

This section provides an overview of the risk management practice and its relation to IR-SIP's project management. Details are to be found in the following sections. The overview of the process will be defined by a process/data flow diagram.

There are four primary activities performed in the risk management practice:

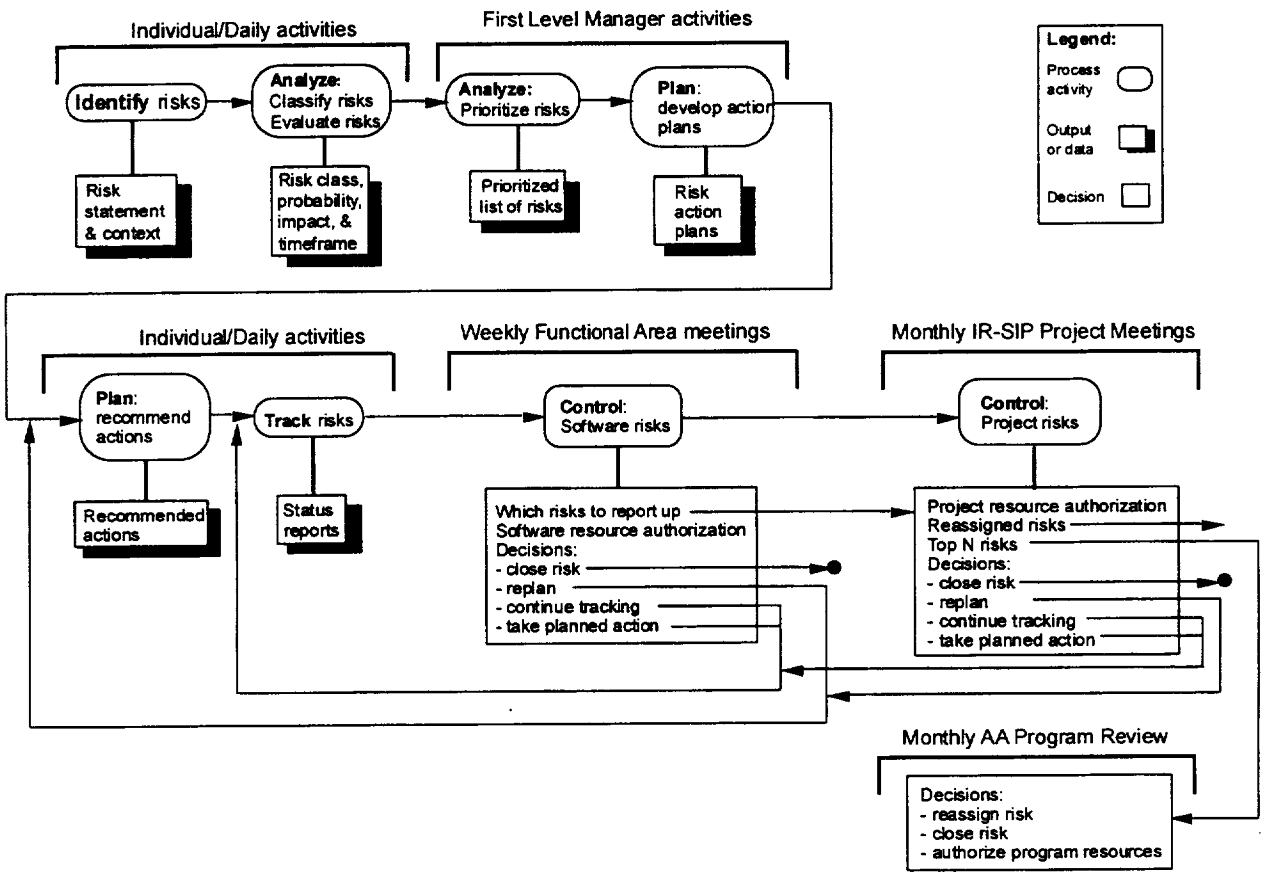
- identification of risks: a continuous effort to identify and document risks as they are found
- analysis of risks: an estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritization of risks relative to each other
- planning risks: decision about what to do with the risks, which, for important risks, will include mitigation plans
- tracking and controlling risks: collection and reporting status information about risks and their mitigation plans (where appropriate) and taking corrective action as needed.

The risk management activities will be carried out during day-to-day activities of project personnel as well as during key project meetings.

Only Top 20% risks shall have any resources expended for mitigation. All non-Top N risks shall be watched or accepted.

2.2 Process and Data Flows

The following diagram depicts the overall process of managing risks on the IR-SIP Project.



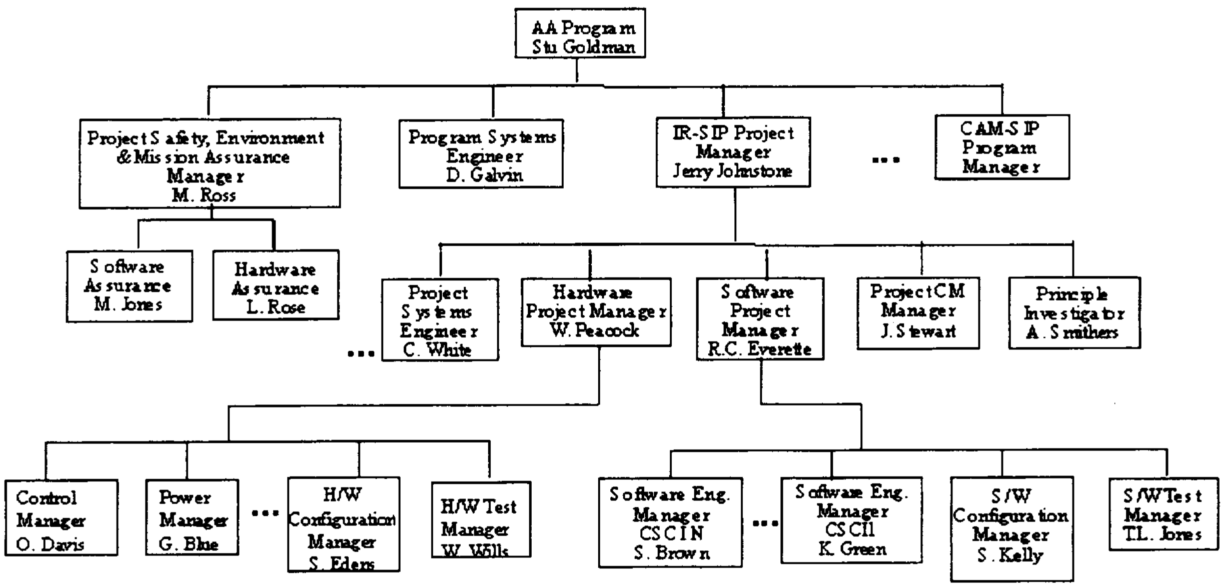
2.3 Project Management Integration (optional)

The IR-SIP Project Management Plan calls for the identification, processing, and documentation of changes and problems to the system. Risks will, in general, be considered an equivalent item to problems and changes in terms of tracking and significance during project meetings. Top 20% risks will be handled similar to critical issues, as documented in the Project Management Plan. Any risk which is also a safety risk will be handled similar to a safety-related problem - referral to the project's safety plan or to the Safety Guidebook *NASA-GB-1740.13-96*.

Section 3. Organization

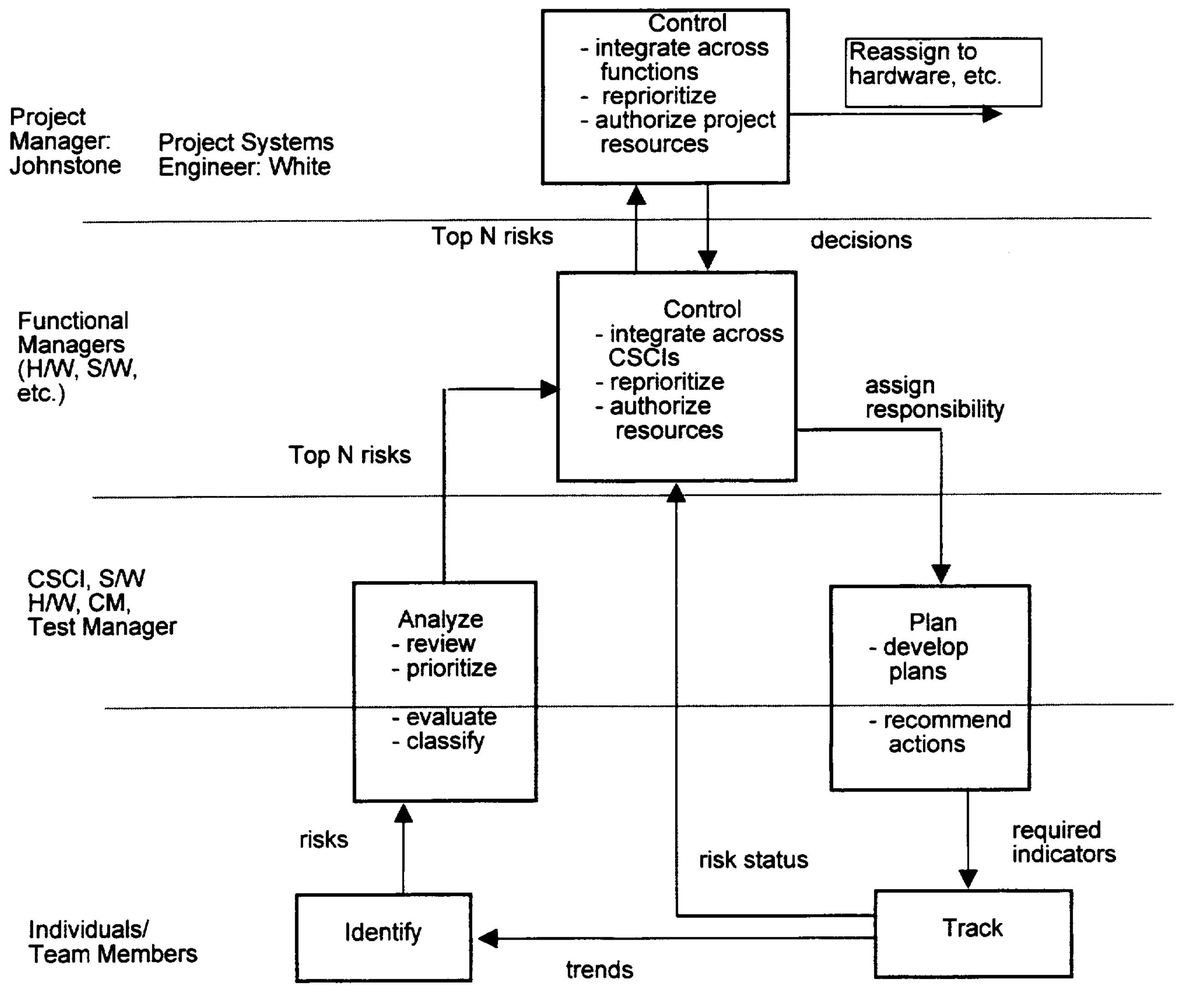
3.1 Project Organization

The IR-SIP project organization is defined in the Project Management Plan and repeated here for convenience.



3.2 Project Communication and Responsibilities

The following diagram introduces the structure of risk communication and responsibility within the IR-SIP organization for conducting risk management activities.



The responsibilities of all project personnel as individuals, the team or technical leads, the function leads, and the project manager are specified in the following table. This table illustrates the type of responsibilities that need to be identified and allocated to the project personnel for the management of risks.

Who	Responsibilities
Individuals	Software/Hardware engineers, testers, leads, and project manager • identify new risks • estimate probability, impact, and timeframe • classify risks • recommend approach and actions • track risks and mitigation plans (acquire, compile, and report)
S/W, H/W, CSCI, CM, and Test Managers	Leads for each CSCI • ensure accuracy of probability/impact/timeframe estimates and the classification • review recommendations on approach and actions • build action plans (determine approach, define scope & actions) • report their Top N risks and issues to the project manager • collect and report general risk management measures/metrics
Software Project Manager, Hardware Project Manager, etc.	• integrates risk information from all technical leads • reprioritizes all risks to determine Top 20% risks in each area (software, hardware, etc.) • makes control decisions (analyze, decide, execute) for risks (e.g., Software Project Manager controls software risks) • authorizes expenditure of resources for mitigation • assigns or changes responsibility for risks and mitigation plans within the CSCI, CM, and test areas • handles communication IR-SIP project manager
IR-SIP Project Manager, IR-SIP Project Systems Engineer	• integrates risk information from all software, hardware, and CM leads • reprioritizes all risks to determine Top 20% project risks • makes control decisions (analyze, decide, execute) for Top 20% project risks • authorizes expenditure of project resources for mitigation • assigns or changes responsibility for risks and mitigation plans within the project (e.g., moving responsibility for a risk from software to hardware) • handles communication with AA program manager • reviews general risk management measures/metrics with Quality Assurance during each quarter to evaluate effectiveness of risk management

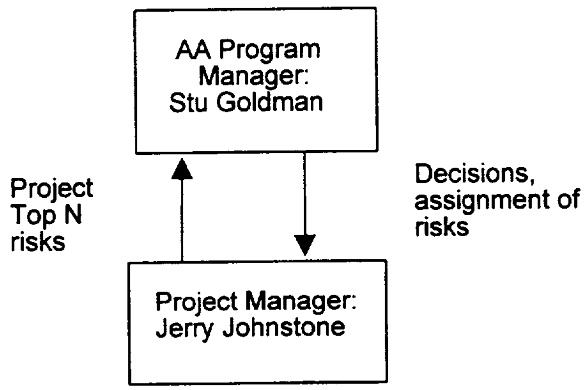
The criteria for communicating risk information is documented in the following table.

Communication Path	Criteria for Selecting Risks and Status Information
Technical leads to Jerry Johnstone	• Top 20% risks for each team • Any risk that impacts launch readiness • Any risk with an impact >10% of budget • Any risk that needs to be transferred to another team
Jerry Johnstone to AA Program Manager (Goldman)	• Top 20% risks in the project • Any risk that impacts the satellite's operation • Any risk with major impact on IR-SIP operations • Any risk that impacts the launch schedule • Any risk that exceeds 25% of the project budget • Any risk that negatively impacts NASA's reputation
Everette to contractor program manager	• Any risk that impacts the contractor's ability to succeed • Any risk that impacts the overall project schedule • Any risk that needs to be transferred or jointly managed by the contractor
Jerry Johnstone to Program System Engineer	• Any risk that impacts the satellite's operation • Any risk that impacts the launch schedule • Any risk that exceeds 25% of the project budget • Information on technical problems that affect the spacecraft or other instruments

3.3 AA Program Responsibilities

If IR-SIP project personnel identify risks that affect the AA Program, it is the responsibility of the IR-SIP Project Manager to notify the AA Program Manager. The AA Program Manager, with the assistance of the change agent P. Stone and the IR-SIP Project Manager, to manage risks transferred to the SE Program level.

The IR-SIP Program manager shall report progress summaries on Top N IR-SIP risks to the AA Program Manager on a monthly basis. The AA Program Manager is responsible for authorizing additional expenditures if requested by the IR-SIP Project Manager and transferring assignments of risks to the IR-SIP Project.



Meeting	Purpose	Method or Tool
Monthly and major milestone AA Program Manager reviews	IR-SIP, CAM-SIP, SPEC-SIP, AA Spacecraft Project Managers, their Systems Engineers, AA Program Systems Engineer, and Safety & Environment Mission Assurance Manager meet with AA Program Manager to review program status and issues. Risk-specific information from each project • new Top 20% risks, any risks that impact the program • status of safety risks • status of all Top 20% risks Status for program risks are reported by the program manager. Decisions and actions include • decisions/resolutions for risks that are not being successfully managed • approval for mitigation plans and resources that exceed normal project limits	Stoplight Charts Risk Information Sheets Cost-Benefit Analysis Safety risk/hazard information

3.4 Contractor Responsibilities

Software Contractor reports to the Software Project Manager. Since the original contract did not call for risk management, risk management performed by the contractor and reported to the Software Project Manager is voluntary. Contractual modifications to install risk management as a part of the contract would result in an update to this part of the Risk Management Plan.

Section 4. Practice Details

This section provides the details about the practice needed to enable project personnel to carry out the risk management activities.

4.1 Establishing Baselines and Reestablishing Baselines

A baseline set of risks was established before this plan was written. That baseline shall be updated or re-established periodically at major project milestones. Risk baseline re-establishment is conducted using the following process.

Step	Action
1	IR-SIP project manager identifies a cross section of project personnel. All levels and disciplines should be represented in this group.
2	Group uses the TBQ Interview method to generate risks in a two-hour session.
3	Group evaluates risks using the Tri-Level Attribute Evaluation method.
4	Group classifies according to source in the Risk Taxonomy.
5	Project Managers and Functional Area Managers prioritize to identify the Top N risks or sets of risks.
6	Project Managers and Functional Area Managers compare Top N risks from this effort to existing Top N risks. Expand project Top 20% risks list to include the rebaselining Top N.
7	Project Managers and Functional Area Managers reprioritize new Top N.
8	Assign new Top N risks to personnel to begin building action plans.
9	Add all other rebaseline risks to the database and determine which ones will need to be transferred, delegated, watched, accepted, or researched.
10	PM distributes rebaseline set of risks listing to the project and asks for additional information from anyone in the project who might know more than what is documented.

4.2 Identifying Risks

All personnel are responsible for identifying new risks. The database can be accessed by anyone at any time to identify new risks. The Short TBQ and project data shall be reviewed twice per month by all project personnel to help identify new risks. Project metrics (as defined by the Goal/Question/Metric method) will be reviewed whenever any predefined thresholds or triggers are reached that would indicate a potential problem (i.e., a risk). Risk statements shall be written according to the format, "condition; consequence." All relevant information shall be captured as context. The risk database shall automatically assign a risk identifier and tag the identifier's name onto the report. The Risk Information Sheet shall be used as the input form for risk information.

Any new risks identified during any project-related meeting shall be added to the database within two working days of the meeting. It is the responsibility of the meeting leader to make sure that this is accomplished.

[Note to students: The actual procedure steps for accomplishing this task would go here - equivalent to the procedure steps listed for re-establishing a baseline.]

4.3 Analyzing Risks

Risk attributes of probability, impact, and timeframe shall be estimated by the identifier of the risk and entered at the same time the risk is identified. If the identifier does not know the value of the estimates, it can be skipped during database entry. The team mangers shall be responsible for reviewing and correcting attribute values for new risks on a weekly basis.

The Tri-Level Attribute Evaluation method shall be used for evaluating attributes. Classification shall be done using risk source according to the Risk Taxonomy. Prioritization shall be accomplished noting that only the Top N risks shall receive mitigation resources. Determination of the number of Top 20% risks to maintain shall be made by the PM and FAMs for the project and the functional area.

[Note to students: The actual procedure steps for accomplishing this task would go here - equivalent to the procedure steps listed for re-establishing a baseline.]

4.4 Planning Risks

All Top 20% risks shall be assigned to someone within the project for responsibility. Accomplishment of actions contributing to the mitigation of the risk may be assigned. Responsibility for a risk means that the responsible person must answer for the status and mitigation of the risk.

Assign responsibility: As newly identified risks are brought to a manager's immediate attention through weekly database reports, the manager shall determine whether or not to keep the risk, delegate responsibility, or transfer responsibility up the project organization. If transferred, the transferee must make a similar decision. The project manager, if necessary, can transfer a risk to the AA Program Manager.

When you are assigned or keep responsibility for a risk: Decide if the risk requires further research (then create a research plan); accept the risk (document acceptance rationale in the database and close the risk), watch (define tracking requirements, document in the database, and assign watch action), or mitigate (create a mitigation plan, assign actions, and monitor the plan and the risk). See Appendix A for standard plan templates. Note that only Top N risks shall be mitigated.

Mitigation plans shall be either an action item list or follow the standard template for IR-SIP task plans. Task plans shall be written for any mitigation effort that requires reallocation of project resources. The project manager shall determine when to use a task plan format.

[Note to students: The actual procedure steps for accomplishing this task would go here - equivalent to the procedure steps listed for re-establishing a baseline.]

4.5 Tracking and Control of Risks

The person responsible for a risk shall provide routine status reports to the Functional Area Managers and PM during weekly Functional Area meetings and the weekly and monthly project meetings. The status for each Top 20% risk shall be reported each week in their respective meetings. Status on all watch lists shall also be reported during the monthly meetings. The Risk Spreadsheet shall be used to report summary status information for risks. The Stoplight Status Report shall be used by the PM to report progress to the AA Program Manager at the program monthly reviews.

[Note to students: The actual procedure steps for accomplishing this task would go here - equivalent to the procedure steps listed for re-establishing a baseline]

4.6 Summary of Methods and Tools

Method or Tool [Guidebook Chapter]	**Use:**
Risk Information Sheet	Used by everyone to document new risks and to add information as risks are managed.
Problem-Solving Planning	Used for developing mitigation plans for complex risks.
Periodic review of project data and the Short TBQ	Used for routine or frequent identification of risks. The short TBQ provides a memory jogger for possible sources of risks and the project data is reviewed with that list in mind.
Goal/Question/Metric for project metrics	Use project metrics to help identify and track risks.
Action Item Lists	Used for developing a list of relatively simple mitigation actions.
Spreadsheet Risk Tracking	Used technical leads to succinctly report current status information about their teams' risks.
Taxonomy Classification	Used when risks are identified as a structure for grouping related risks. Technical leads use this to help eliminate duplicate risks and combine related mitigation plans.
Tri-Level Attribute Evaluation	Used when risks are identified to evaluate probability, impact, and timeframe. Also helps level the risks into those that might be important enough to be considered Top 20% risks (filters out the less important risks). Safety risks are evaluated according to the Safety Handbook.
Multivoting	Used by technical leads and project manager to isolate the Top 20% risks, which will get mitigation resources.

Section 5. Resources and Schedule of Risk Management Milestones

Resources for the management of risks are broken into two categories:

- overhead costs associated with the risk management process: 00.05% of the project budget
- mitigation plan costs: resources associated with mitigation plans, specifically those with task plans

Budget allocation for mitigation plan development and execution is initially set at 1% of the project budget, with equal portions of that distributed to each functional area. Each Functional Area Manager is responsible for managing their mitigation budget. Any requirements for additional mitigation resources must be made to the Project Manager.

Milestones

- Weekly project and functional area meetings shall include statusing of risks.
- Monthly project meetings shall include statusing of risks.
- Top 20% risk status shall be summarized and reported to the AA Program Manager on a monthly basis.
- The baseline set of risks shall be re-established on a project milestone basis.

Section 6. Documentation of Risk Information

All risk information shall be documented in the risk database. The risk database is accessible by all project personnel for the purpose of identifying new risks. Once a risk has been assigned to someone, then only that person shall have the authority to update the risk information. The Risk Information Sheet for any risk can be printed by whomever is assigned to the risk. Spreadsheets and Stoplight Status Reports can only be printed by the Program Manager, Functional Area Managers or their designated assistants.

The responsible person must document lessons learned before closing the risk. Those lessons learned must be reviewed and approved by whoever is assigned closing authority for the risk before the risk can be officially closed within the database.

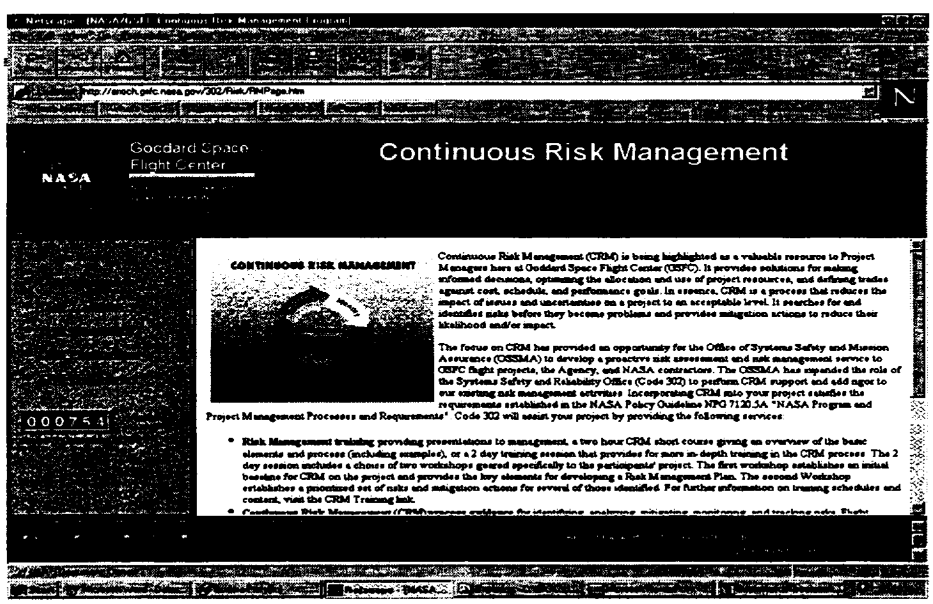
The IR-SIP database is being provided at no cost by the SR & QA office. Assistance in maintaining and modifying the database is also being provided at no cost, provided it does not exceed two hours per week. Any additional needs must be negotiated between the IR-SIP PM and the SR & QA director.

Exercise - Sample Implementation Plan

IR-SIP's Implementation Plan can serve as DID, with example text, for your project to use.

Take 5 Minutes to read the IR-SIP Implementation Plan, then we will walk through it.

http://arioch.gsfc.nasa.gov/302/Risk/RMPage.htm



Case Study

Implementation Plan

for Installing

Risk Management Practice in IR-SIP

Baseline Date:
Last Modified:
Owner:
Co-owners:
Purpose:

Section 1. Sponsorship
- *1.1 Sponsorship Roles and Responsibilities*
- *1.2 Reporting Requirements*
- *1.3 Sponsorship changes*

Section 2. Roles and Responsibilities
- *2.1 Infrastructure Roles to be Filled*
- *2.2 Project Personnel roles*

Section 3. Schedule of Activities
- *3.1 Detailed Transition Schedule Milestones*
- *3.1.1 Basic Risk Management Practice Phase*
- *3.1.2 Improvement Phase*

Section 4. Allocated Budget and other Required Resources
Section 5. Evaluation Measures and Completion Criteria
Section 6. Risks and Mitigation Strategies for this Implementation Effort
Section 7. Establish Risk Baseline Method

Case Study
Implementation Plan
for Installing
Risk Management Practice in IR-SIP[1]

Baseline Date: 9/10/95

Last Modified: 2/1/96

Owner: J. Johnstone/IR-SIP Project Manager

Co-owners: R. Douglas/Manager SR & QA Office

Purpose: This plan documents how the practice of risk management will be designed and installed into the IR-SIP project. It does not specify what IR-SIP's actual risk management practice is, only the process for putting it in place.

Section 1. Sponsorship

Sponsorship for this effort is being supplied by Jerry Johnstone, as project manager for IR-SIP; Stu Goldman, as program manager for the AA Program; and R. Douglas, manager of the SR & QA office of this organization. Expansion of risk management into the rest of the AA Program is dependent upon the success of the IR-SIP implementation.

1.1 Sponsorship Roles and Responsibilities

The sponsors shall provide continual, visible support for this effort at all levels of the organization. This shall include the following:

- Goldman's report of status at the quarterly site Management Review
- All three sponsors' written endorsement and encouragement of this effort to all IR-SIP project personnel
- All three sponsors' attendance at first kick-off meeting with IR-SIP personnel and periodic attendance at IR-SIP Monthly meetings
- Monthly status meetings held with all three sponsors and change agent P. Stone.
- All sponsors shall allocate budget to this effort as specified in Section 4.
- Any further supportive announcements or activities as recommended by P. Stone.

1.2 Reporting Requirements

The IR-SIP Project Manager shall make monthly progress reports on the success/difficulties of implementing risk management (see Section 6, Risks and Mitigation Strategies for this Implementation Effort). Requests for assistance from SR & QA in the form of training, process definition and improvement, etc. should be made on an as-needed basis. Status reports shall include evaluation of progress measures of the implementation effort as well as a summary listing of all risks in the project. Use of the center-standard risk database is required. Roll-up of all project risk data into the center database is required on a quarterly basis.

[1] Note: Another name for an implementation plan is transition plan.

1.3 Sponsorship changes

In the event of personnel changes in the sponsors, this implementation plan must be re-evaluated and reapproved. Summary reports of progress to date may be required from the project manager.

Section 2. Roles and Responsibilities [updated 9/20/95]

This section identifies the roles and associated responsibilities for this transition effort. Note that one person may fulfill multiple roles. Sponsors were identified in the previous section.

2.1 Infrastructure Roles to be Filled

These roles need to be filled in order to support the transition of risk management into the IR-SIP Project. The same personnel may be required to continue these roles if risk management is later rolled out to other parts of the AA Program.

- Champion: Someone from within the project, preferably from the managerial level, to provide motivation and leadership. This person will be responsible for encouraging and reinforcing the proper management of risks and open communication of risks as part of his/her routine activities, and assisting in the periodic evaluation of this transition effort.
    - Assigned to: R.C. Everette
- Change agent: Expected to be provided from the local software working group representatives (must be from outside the project/program). This person will be responsible for coaching project personnel in the accomplishment of risk management activities. Estimated time requirements are 10 hours per week, on average. Will also train project personnel in the tailored risk management practice and assist the champion and program manager in locating tool training (as needed). This person should have training and leadership skills.
    - Assigned to: P. Stone (SWG member)
- Facilitation team: Require two from outside the project and two from inside the project. Facilitation skills are needed or training must be provided. At least two members of this team should be experienced facilitators. Facilitators will be called upon to help the project whenever facilitation is required to handle issues or carry out specific methods or procedures that require a facilitator. This team will also assist in the establishment of the risk baseline. Estimated time commitment: Baseline establishment - two person weeks each; routine assistance - one hour/week each (on average) but expect a higher peak in early phases.
    - Assigned to: P. Stone, J. Douglas/SWG; Blue/software engineer, L. Jason (quality assurance). All four of these individuals are already trained facilitators and have committed their time and effort. Everette and M. Jones have agreed to allow the IR-SIP project individuals to fulfill these roles. Stone's and Douglas' managers have also committed to supporting this effort.

2.2 Project Personnel roles

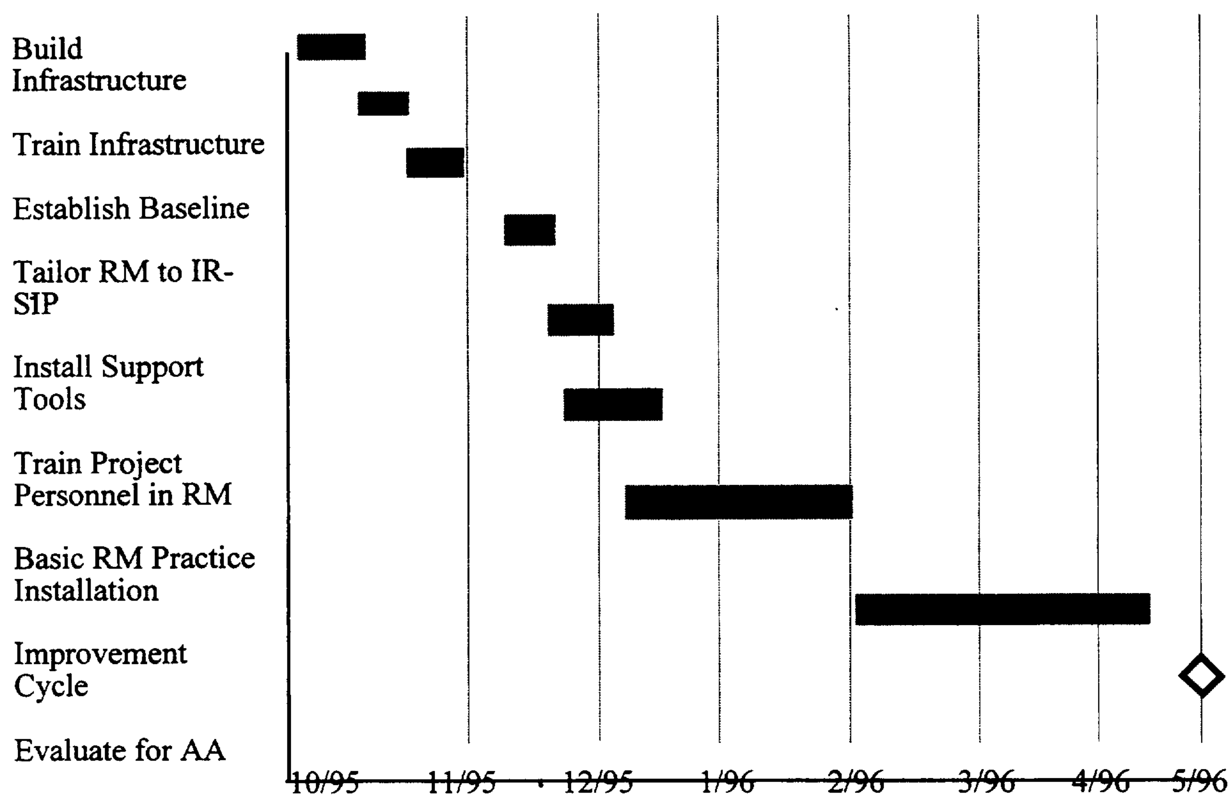
These are the roles and responsibilities of the IR-SIP project personnel.

- Take risk management training: When training in tailored risk management practice for IR-SIP is made available, all project personnel are expected to take the training.

Schedule allowances will be made by the project manager to accommodate near-term deadlines.

- Conduct risk management activities: Project personnel are expected to carry out the risk management activities that are defined in the IR-SIP Risk Management Plan once it has been generated.
- Facilitation team members (see Section 2.1): Two project personnel will be assigned to this team. Work allocations will be adjusted by management to accommodate duties.
- The initial entry of baseline risk information into the database shall be performed by G. Whitley under guidance of a SR & QA representative and the change agent, P. Stone.
- It is expected that all project personnel will participate in the performance of risk management activities. Data entry for the database shall be carried out by anyone identifying a new risk or whoever is responsible for the risk.
- Stone will serve as a general source of risk management expertise during this period. The facilitation team members will continue to provide facilitation on an as-needed basis.

Section 3. Schedule of Activities **[updated 2/1/96]**



3.1 Detailed Transition Schedule Milestones *[added 11/16/95]*

The initial milestones for developing a risk management plan are

- Document draft IR-SIP risk management plan (the tailored practice for IR-SIP): 11/15/95
- Final IR-SIP risk management plan: 11/20/95

3.1.1 Basic Risk Management Practice Phase

The basic risk management practice to be installed first includes the following:

- all risk management activities at all levels of the IR-SIP project organization
- database installed, tested, and all forms and templates to support the methods and tools incorporated

The methods and tools to be used include everything but the mitigation status report and stoplight status report, which shall be held for later.

- Although risks can be transferred to the AA Program Manager, there is no implied responsibility on the part of the AA Program Manager to provide data for the database. The IR-SIP PM shall assign the task of entering any risk data from the AA Program Manager.

The detailed milestones for installing the basic practice are as follows:

- Prototype risk database from SR & QA is installed and tested: G. Whitley: 11/18/95.
- Tailored risk management training is developed by P. Stone and facilitation team: 11/30/95.
- All project personnel are trained on risk database and tailored risk management process: 12/15/95.
- All top baseline risk areas have completed mitigation plans; plans are in place and in progress: 12/4/95.
- Individual access to database for risk identification is available and is being used: 12/1/95.
- Weekly status meetings include risk as discussion topic using spreadsheet: 12/18/95.
- All risk information is being maintained in the risk database and risk information sheets are used as individual risk reports: 12/20/95.
- New risks are being prioritized and action plans are being built: 12/30/95.
- Progress Evaluation Points: 11/20/95, 12/20/95

3.1.2 Improvement Phase

The following will be implemented during the improvement cycle.

- Monthly status meetings are using Stoplight Status Reports to indicate Top N risk status from IR-SIP PM to AA PM.
- Mitigation Status Report is used for one of the top risks (provided its use is justified) by 3/1/96.

- Response time of database is improved by purchase of latest set of fixes from vendor. Need site license. Expected by 3/20/96.
- Ability exists when printing risk spreadsheets to filter out risks not assigned to anyone in a specific work group.
- New trending report is added to show average time required to close a Top N risk; average time Top N risk spends on watch list before final closing; average time to build mitigation plan; distribution of risks to responsible person (3/10/96).
- AA viable procedure is tested for calculating actual mitigation costs against potential loss due to the risk (4/15/96).

Progress evaluation points: 1/20/96, 2/20/96, 3/20/96, 4/20/96, 5/1/96.

Based on evaluation, Stone and Johnstone present findings to other sponsors on 4/30/96. Decision on whether or not to use risk management on the rest of the AA Program will be made at that point.

Section 4. Allocated Budget and other Required Resources [updated 2/1/96]

Funding is provided at the following levels:

- SR & QA: $10,000 for tools and training, additional $3,000 for database upgrade and site license
- AA Program: 0.5% of the program budget for FY96
- IR-SIP: 1% of the project budget

Section 5. Evaluation Measures and Completion Criteria [updated 2/1/96]

This risk management transition effort will be considered a success if the following outcomes have been met:

1. An effective risk management practice is in place in the IR-SIP Project (document any major problems averted through management of risk in lessons learned part of risk database - collect for evaluation points as part of judging effectiveness of practice).
2. AA Program management agrees to transition risk management to the rest of the AA Program.

Measures to be used to evaluate the first outcome are

- the number and severity of problems discovered late in the development lifecycle has decrease by at least 80%
- 80% of project personnel and all managers find risk management has improved their ability to manage their tasks and make the right decisions
- majority of project personnel do *not* find the practice to be unduly burdensome or inefficient
- the estimated savings due to problems that were avoided is approximately equivalent to the resources invested in risk management by the IR-SIP project.

Section 6. Risks and Mitigation Strategies for this Implementation Effort [updated 11/1/95]

The following are the risks that the sponsors recognize as associated with this effort. Contingency or mitigation actions are also described.

1. Too resource intensive: Resources used to perform risk management will be estimated and tracked. If resource usage exceeds 5% of personnel time on average with no visible benefit (in terms of significant problems avoided or reduced) by the first evaluation point, then the sponsors will revisit their decision to use risk management on this project.
2. Ineffective basic risk management practice: If the tailored risk management practice designed for the project proves to need improvements or changes to more than 50% of it after two months of use, then the sponsors will revisit their decision and determine if a second attempt at tailoring the process is needed or if it is now too late to complete this effort with IR-SIP project.
3. Unmotivated project personnel: The project personnel may find this too burdensome and not see the long-term benefits. Mitigation: Will brief the entire project early on to introduce the concept of risk management and demonstrate the sponsorship this effort has. Adjust project schedule, if needed, to allow for start-up time. Need to make sure people do not think more work is being piled on with no extra time to accomplish this. Sponsors/project manager need to stay alert to this issue.
4. SR & QA database may not be useful. If it is not, the implementation schedule in this plan will slip by at least three weeks while we build an appropriate risk database. Testing on the SR & QA database will begin as soon as possible, using their equipment while waiting for the database to be installed on IR-SIP's equipment. This should provide an answer on the database's effectiveness a week sooner.

Section 7. Establish Risk Baseline Method [updated 9/27/95]

P. Stone has already been trained in conducting the Software Engineering Institute's method for establishing a baseline set of risks and has trained the other members of IR-SIP's facilitation team. The methods to be used include the following, taken from the Software Engineering Institute's *Continuous Risk Management Guidebook*:

- SEI Risk taxonomy-based interviews to be conducted with peer groups selected by Stone and Johnstone
- Tri-level attribute evaluation
- Classification by source using the taxonomy
- Prioritization using multivoting
- Planning the top three or four risk areas using problem-solving planning

The Facilitation team will be led by Stone and will turn over all results to Johnstone, who will also report a summary of the results jointly with Stone to Goldman and R. Douglas (the other sponsors).

Lessons learned from this baselining process will be used during the tailoring step to help tailor a more suitable process for these types of projects. Lessons learned will be documented by Stone and will be supplied to the sponsors.

Third - Establish a Risk Baseline

Purpose:

- generate a critical mass of project risks (motivation to manage risks)
- begin the practice of Continuous Risk Management

Description: A risk baseline should have

- a list of risks (statements and contexts)
- risk probability, impact, and timeframe
- sets of related risks
- prioritized risks based on project importance
- plan of action for Top N risks/sets of risks

You also need . . . Training and Project Familiarization

Purpose:

- ensure that members have information necessary to support the project roles
- provide skills to use & implement the chosen tools
- equip the team members with needed skills to establish a risk baseline
- implement regular reviews of project risks
- establish a common vision of CRM

Act to -
Install Basic Practice

Purpose:
- install a basic set of activities that addresses all phases of the risk management paradigm
- start simple and add complexity later

Description:
- involves establishing the basic set of risk management activities as defined in the implementation plan

Act to -
Improve CRM

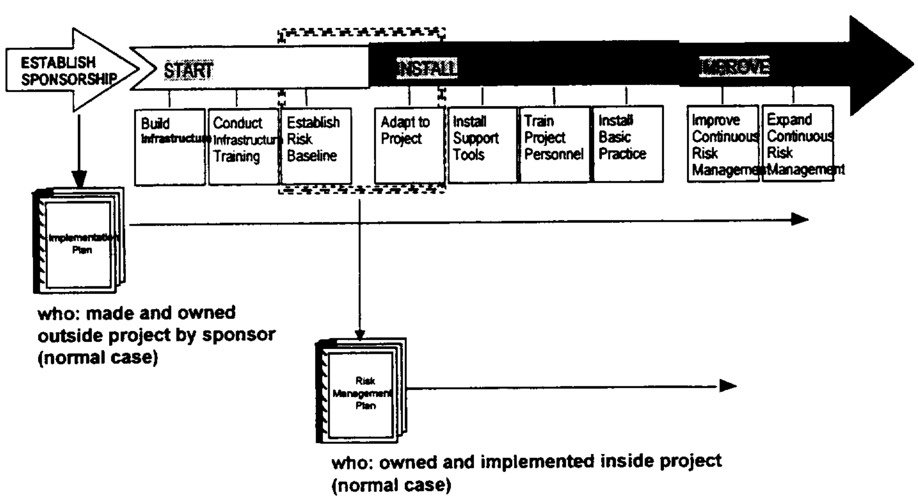
Purpose:
- improve the basic Continuous Risk Management practice implemented during the Install phase

Description: involves adding improvements
- better match routine project management practice
- increase efficiency of risk management activities
- increase the forward-looking viewpoint

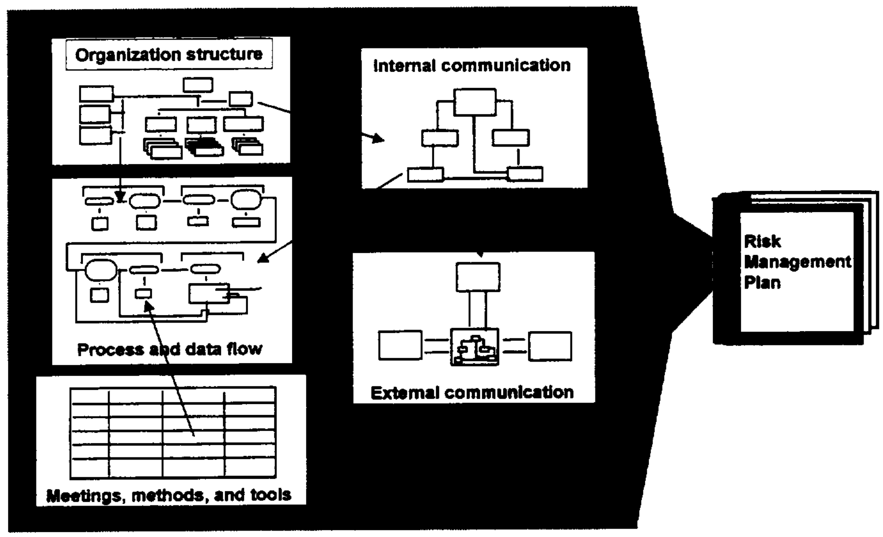
Hints and Tips

- Start simple; learn to "think risk."
- Never throw out or ignore any risk information; scan it once in a while.
- Always ask for feedback on how things are going and what works.
- Use outside facilitators until you're comfortable with the processes.

Continuous Risk Management Roadmap



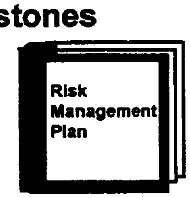
Summary -1



Summary -2

IR-SIP's Risk Management Plan describes how IR-SIP will perform it's tailored risk management process, methods, and tools

- introduction
- practice overview
- project organization, roles, and responsibilities
- practice details
- risk management resources and milestones
- risk information documentation



Summary -3

Adapt risk management to your project.

Document your practice and rationale.

You will change and improve your risk management practice as you gain experience and learn from others' experiences.

Summary - Life-Cycle of a Risk

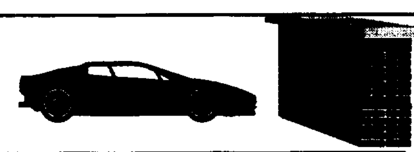
Eventually risks go away
- probability or impact goes to zero
- risk becomes a problem

Documenting the life cycle of risks
- helps you learn what worked and didn't work
- should help you avoid similar difficulties
- provides the opportunity to help other projects learn from your experience

Watch Out for . . . Barriers - 1

Resistance	*Answer*
I don't have the time. There's too much regular project work to do.	If you don't take the time now, you'll take more time later to fix problems you could have prevented.
It's not rewarded. Nobody wants to hear about what we can't do.	Sponsors and management must be prepared to reward behavior they want to see.
It's a bureaucratic nightmare. The processes are too complicated and time consuming.	It's most successful when it's tailored to the project management processes. Start simple and improve with time.
I don't want to look stupid, especially in front of upper management.	Sponsors and managers should educate the project about what is expected.
We already know our risks. We did an assessment at the beginning of the project. Once is enough!	Has anything changed since you identified those risks? If so, then the risks are not the same.

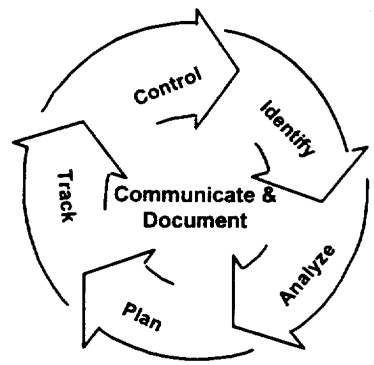
Watch Out for . . . Barriers - 2



Resistance	*Answer*
This is just another management initiative. I'll wait to see if they're serious before I put any effort into it. Why waste time and energy?	It's a valid question, but, if no one else improves, is that a valid reason for you not to improve? Don't you want to be better than your competition?
They shoot the messenger. If I had a solution I wouldn't need to bring it up in the first place.	Sponsors and managers must encourage a risk-aware culture. Work with project personnel to identify potential solutions and choose one. Reward risk identification.
Identifying risks means you need to solve them. We already have enough to do.	Again, if you don't take the time now, you'll take more time later to fix the problems you could have prevented.

Module 10

Course Summary



Overview

Course objectives

Definition of Risk

Risk and Project Management

Continuous Risk Management

Risk Management Planning

Risk Management Implementation

Guidebook

Course Objectives

Understand the concepts and principles of Continuous Risk Management and how to apply them

Develop basic risk management skills for each function of Continuous Risk Management

Be able to use key methods and tools

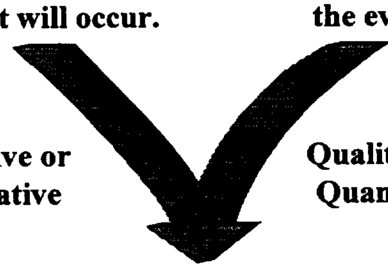
Be able to tailor Continuous Risk Management to a project

Definitions of Risk

Risk always involves the <u>likelihood</u> that an undesired event will occur.

Risk should consider the <u>severity of consequence</u> of the event should it occur

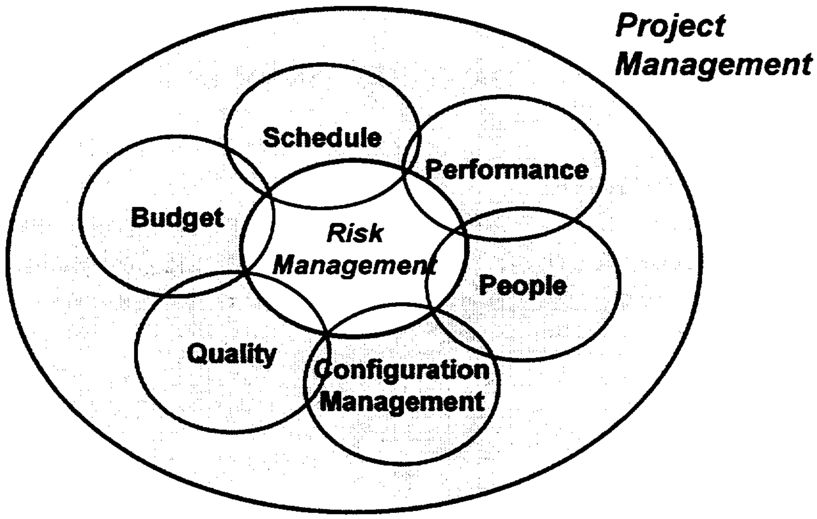
Qualitative or Quantitative



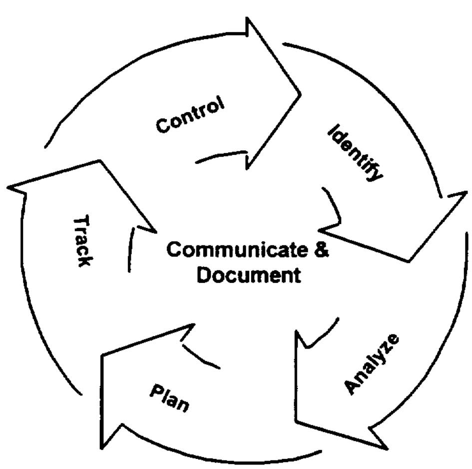
Qualitative or Quantitative

Risk = Likelihood * Severity

Risk Management & Project Management



Continuous Risk Management



1 - Identify

Purpose:
- search for and locate risks before they become problems

Description:
- the process of transforming uncertainties and issues about a project into distinct (tangible) risks that can be described and measured

Risk Statement & Context

$\boxed{\text{Condition;}} \rightarrow \boxed{\text{Consequence}}$
Risk Statement

A good risk statement
- contains one condition
- contains at least one consequence
- is clear and concise

Good context
- provides additional information not in the risk statement
- ensures that the original intent of the risk can be understood by other personnel, particularly after time has passed

2 - Analyze

Purpose:
- **convert risk data into evaluation information**

Description:
- **the process of examining the risks in detail to determine the extent of the risks, how they relate to each other, and which ones are the most important**

Analysis Activities

Evaluate:
- impact (I)
- probability (P)
- timeframe (T)

Risk	I	P	T
Risk a	M	M	F
Risk b	M	L	N
Risk c	L	H	N
. . .			

Consolidate risks

Classify:
- identify duplicates
- consolidate risks to sets

Risk	I	P	T
Risk set A	H	M	F

Risk b	M	L	N
Risk c	L	H	N
. . .			

Sort by evaluation results

Prioritize:
- identify Pareto top N
- rank top N

	Risk	I	P	T
Pareto top N	Risk n	H	H	N
	Risk s	H	M	N
	Risk set A	H	M	F

	Risk c	L	H	N

Rank order the Pareto top N

Top N
1.
2.
3.
. . .

3 - Plan

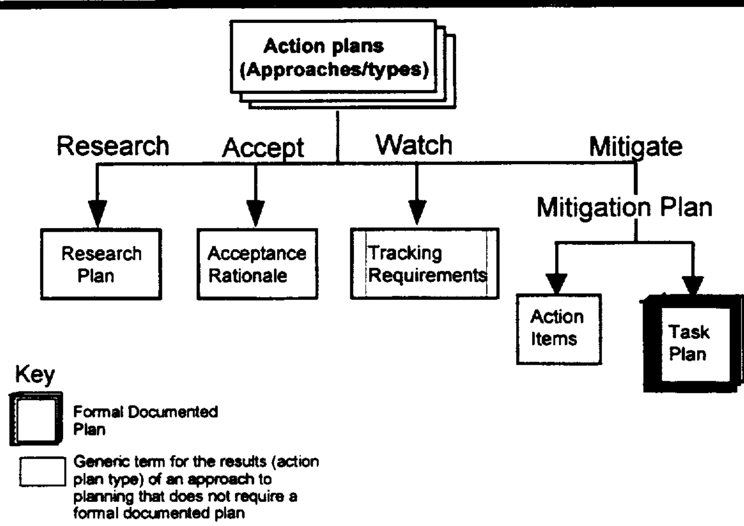
Purpose:

- **translate risk information into planning decisions and mitigating actions (both present and future), and implement those actions**

Description:

- **the process of deciding what, if anything, should be done about a risk or set of related risks**

Action Plan Approaches

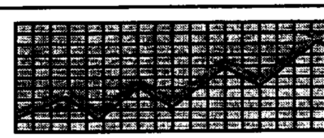


4 - Track

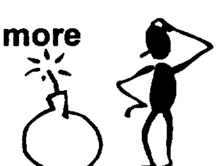
Purpose:
- monitor risk indicators and mitigation actions

Description:
- the process in which risk status data are acquired, compiled, and reported

Risk Metrics



- Measure attributes of a risk
  - impact, probability, and timeframe
  - other risk-specific attributes
- Assess the impact or success of a mitigation plan
- Are chosen during planning
- Provide meaningful information to enable more informed control decisions



Triggers
- provide early warning of an impending critical event
- indicate the need to implement a contingency plan to preempt a problem

5 - Control

Purpose:
- make management decisions based on current information.

Description:
- the process that takes the tracking status reports for the project risks and decides what to do about risks based on the reported data

Control Activities

Evaluate - use tracking data to examine project risks for trends, deviations, anomalies, and identifying new risks.

Decide - use tracking data to determine how to proceed with project risks
- close
- continue tracking and executing the current plan
- replan
- invoke a contingency plan

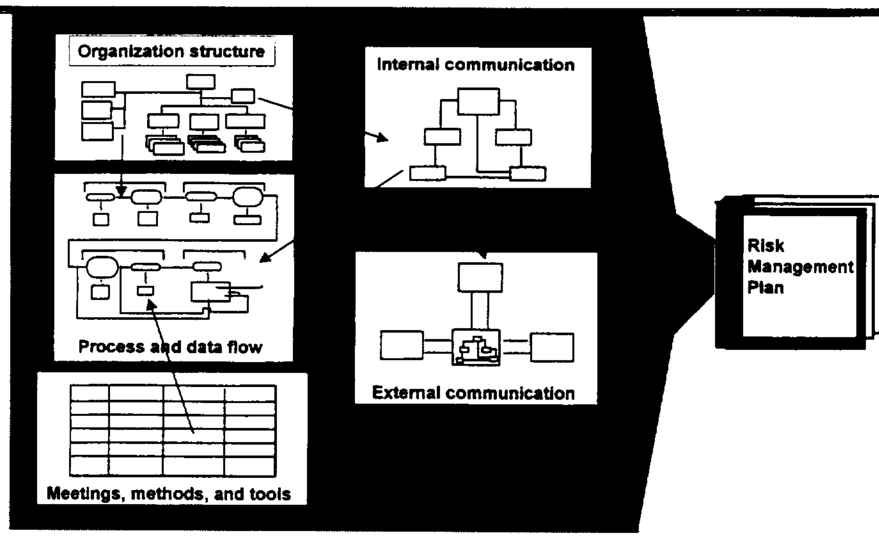
Execute - implement control decisions

6 - Communicate & Document

Purpose:
- provide information and feedback to the project on the risk activities, current risks, and emerging risks

Description:
- a process in which risk information is conveyed between all levels of a project team

Risk Management Planning - 1



Risk Management Planning - 2

A Risk Management Plan describes how the project will perform it's tailored risk management process, methods, and tools

- introduction
- practice overview
- project organization, roles, and responsibilities
- practice details
- risk management resources and milestones
- risk information documentation

Risk Management Implementation

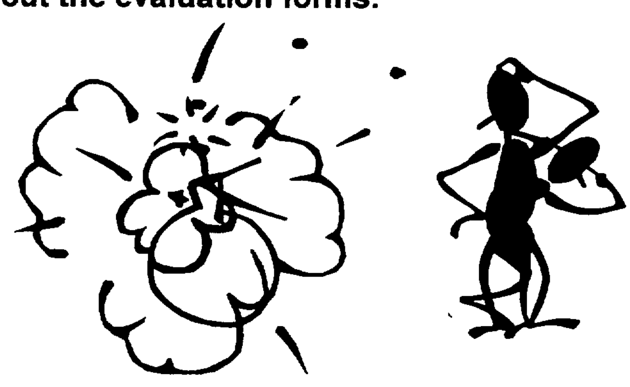
- Start as early as possible in the Project's life.
- Sponsorship and change agents are important.
- A risk baseline gives the process a place to start.
- Resources and Planning are needed to get going.
- An implementation plan shows the steps to get Risk Management up and running.

Final questions?

Course Feedback

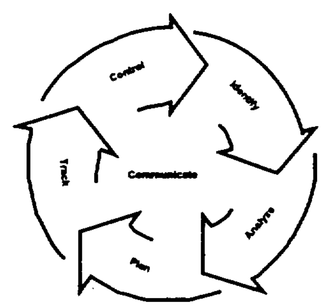
Thank you for attending!

Please fill out the evaluation forms.



Translation Guide

Description: The following tables provide a crossreference between terminology in the *Continuous Risk Management Guidebook* and the proposed risk management section 4.3 of NHB 7120.5 *Management of Major System Programs and Projects Handbook.*

Topic	NHB 7120.5 (proposed)	CRM Guidebook
Definition of Risk	A qualitative or quantitative probability that a program/project will experience undesired consequences such as failure to achieve a needed technological breakthrough, cost overrun, schedule slippage, or safety mishaps. Primary risk drivers are undesirable events whose probability is more likely than "remote" and whose consequences could pose a significant threat to mission success. Primary risk drivers typically fall into the following categories: • performance requirements and mission objectives • technology readiness • safety, reliability, maintainability, quality assurance, environmental protection • cost and schedule	The possibility of suffering loss. In a development project, the loss describes the impact to the project, which could be in the form of diminished quality of the end product, increased costs, delayed completion, or failure. A statement of risk describes: • condition: the key circumstances, situations, etc., causing concern, doubt, anxiety, or uncertainty • consequence: the key, possible negative outcome(s) of the current conditions
Risk Management	Risk management covers the identification, assessment, mitigation, and disposition of risks at each stage of the life cycle. In particular, risk management begins with an identification of the general risk issues and concerns, based on program objectives and constraints. From these considerations, a plan is developed; followed by an assessment of specific risks.	The Risk Management Paradigm illustrates a set of functions that are identified as continuous activities throughout the life of a project. 

Topic	NHB 7120.5 (proposed)	CRM Guidebook
Identifying, Assessing, and Mitigating Risks	Risk assessment • identify primary risk drivers • estimate probability of occurrence • determine primary consequences given occurrence • assess cost and schedule impacts • mitigate technical, schedule, and cost risks	Identify: • capture statement of risk • capture context of risk Analyze: • evaluate attributes (impact, probability, timeframe) of risks [qualitative or quantitative] • classify risks • prioritize (rank) risks Plan • assign responsibility (keep, delegate, transfer) • determine approach (research, accept, mitigate, watch) • define scope and actions
Tracking and Controlling Risks	A risk driver will be considered "controlled" or "retired" when any of the following conditions are satisfied: • risk mitigation options that reduce the probability of occurrence to "remote" have been planned and will be implemented • all reasonable mitigation options (within cost, schedule, and technical constraints) have been instituted, and all risk drivers determined to be more likely than "remote" have been judged by the appropriate PMC to be "accepted" • reserve funds are available so that, should the risk actually occur, resources would be available to recover from cost, schedule, and technical impact	Track • acquire tracking data • compile tracking data • report tracking data Control • analyze status reports • decide how to proceed • execute decisions Considerations for closing a risk include • when the probability, impact, or risk exposure are either near zero or below an acceptable threshold as defined in the mitigation goal. The risk is considered to have been successfully mitigated. • when conditions have changed such that the risk is no longer relevant to the project • when a risk becomes a problem and must be tracked as such

Topic	NHB 7120.5 (proposed)	CRM Guidebook
Risk Management Plan	This plan guides the future risk disposition activity. This plan should include • risk management responsibilities, resources, schedules, and milestones • methodologies, processes, and tools to be used for risk identification, risk analysis, assessment, and mitigation • criteria for categorizing or ranking risks according to the probability and consequences; e.g., risk matrix • role of risk management with respect to decision-making, formal reviews, and status reporting • documentation requirements for risk management products and actions	This plan describes the risk management practice (processes, methods, and tools) to be used for a specific project. Contents include • introduction to plan and why it exists • overview of processes and how they relate to project management • the project's involvement in carrying out risk management • details of each major activity and how it's to be used • schedule, milestones, and resources required • how risk management information is documented, retained, controlled, and used
Risk Information	For each primary risk driver, the program/project should be prepared to present the following information • description of risk driver including primary causes and contributors to the risk • estimate of the probability (qualitative or quantitative) of occurrence, together with the uncertainty of the estimate • primary consequences should the undesirable event occur • significant cost impacts given its occurrence • significant schedule impacts given its occurrence • potential mitigation measures • implemented mitigation measures, if any • characterization of the risk driver as "acceptable" or "unacceptable" with rationale •	Risk Information Sheet: used to document information about a risk • unique identifier for risk • date risk was identified • statement of risk • context (associated information) that clarifies the risk • organization or person who identified the risk • priority ranking of the risk • likelihood of occurrence • degree of impact • timeframe in which the risk will occur or action is needed • classification of the risk • who is responsible for mitigating the risk • the selected strategy for mitigating the risk • a contingency plan, if one exists, and the event or time that triggers it • running status that provides a history of what is being done for the risk and changes to the risk • approval for mitigation strategies or closure • date when the risk was closed • rationale for closure of the risk

Software Risk Checklist

The following is a software risk checklist. It is organized by development phases of a project, with emphasis on the software portion of the overall project lifecycle. Listed here are _some_, not an exhaustive list, of the generic risks that should be considered when any project contains software. This checklist contains practical questions that were gathered by experienced NASA engineers and is not a part of the SEI course or guidebook. The SEI has their own taxonomy-based questionnaire that should be considered during any risk assessment (SEI *Continuous Risk Management Guidebook* chapters A-32 to A-34, pg. 471-509).

The project manager, software manager, system engineer/manager, any software technical leads, and the software engineers, as a minimum, should review, fill out, and discuss the results of this checklist. Taking into account all the different perspectives and adding risks specific to a project, the review team should then meet to create an agreed-upon set of risks and start planning how they will be addressed. This checklist is only an aid to start the managers and engineers thinking and planning how to realize, avoid, mitigate and accept the risks inherent in any software project. The first step to controlling a project is understanding where it may go out of control and plan to avoid it as much as is possible. As this risk checklist covers many lifecycle stages, it is suggested that this checklist initially be used during systems requirements to establish a baseline risk assessment. At that time, the entire risk checklist should be gone through and an initial risk assessment should be generated. These risks can then be documented in a risk database and/or a risk mitigation plan. Once this initial baseline risk assessment has been created, the project should revisit the risk checklist during each subsequent lifecycle stage in order to see if new risks have been discovered or if issues not previously understood to be a risk now need to be elevated to a risk. If the project is using rapid prototyping, the spiral lifecycle, or some other iterative lifecycle, then period at which the list will be revisited should be established at the beginning of the project and followed throughout. The software management plan or software risk management plan would be the appropriate place to document the entire risk approach, schedule and process.

The checklist is laid out with the generic risks listed followed by a column to indicate if this is a risk for a particular project. **Y**es, this is a risk; **N**o, not a risk for this project at this time; **P**artially a problem as stated, further clarification should be added. The last column is to indicate if this risk should be accepted or needs to be worked, i.e. the risk needs to be researched, mitigated, or watched. (See the SEI *Continuous Risk Management Guidebook* page 63.)

Remember, this checklist is not an exhaustive list of all possible generic risks. It is meant to generate ideas and is **_not_** meant to be a complete list of all potential risks that could be considered. The user should consider the checklist, along with the Taxonomy Based Questionnaire provided in the SEI *Continuous Risk Management Guidebook* (Chapters A-32 to A-34, pages 471-509), as a basis for starting to examine possible risks on a project. The risk checklist should be added to, and tailored, to fit a project/program's needs. Sometimes the wording on the questions contained in the checklist are open-ended in order to get the project team to think beyond what is written.

Also remember, not all risks are technical. Development environment, schedule, resources, etc. all have risks that need to be considered.

System Requirements Phase	RISK Yes/No /Partial	ACTION Accept/ Work
Are system-level requirements documented? To what level? Are they clear, unambiguous, verifiable ?		
Is there a project-wide method for dealing with future requirements changes?		
Have software requirements been clearly delineated/allocated?		
Have these system-level software requirements been reviewed, inspected with system engineers, hardware engineers, and the users to insure clarity and completeness?		
Have firmware and software been differentiated; who is in charge of what and is there good coordination if H/W is doing "F/W"?		
Are the effects on command latency and its ramifications on controllability known?		
Is an impact analysis conducted for all changes to baseline requirements?		

Software Planning Phase	RISK	ACTION
Is there clarity of desired end product? Do the customer & builders (system and software) agree on what is to be built and what software's role is?		
Are system-level requirements on software documented? Are they complete/sufficient and clearly understood?		
Are all interface requirements known & understood?		
Are roles and responsibilities for system & software clearly defined and followed and sufficient?		
Have the end user/operator requirements been represented in the concept phase such that their requirements are flowed into the software requirements?		
Has all needed equipment, including spares, been laid out? and ordered? Is there sufficient lead time to get needed equipment? Is there a contingency plan for not getting all equipment? Is there a contingency plan for not getting all equipment when needed?		
Is the needed level of technical expertise known?		
Is the level of expertise for software language, lifecycle, development methodology (Formal Methods, Object Oriented, etc.), equipment (new technology), etc. available: within NASA? from contractors? Will expertise be available as the schedule demands? Is there more than one person with a particular expertise/knowledge (i.e. is too much expertise held by only one team member? What if they quit, or get sick?)		
Training: Is there enough trained personnel? Is there enough time to train all personnel? on the project itself? on equipment/ software development environment, etc.? Will there be time and resources to train additional personnel as needed?		
Budget: Is the budget sufficient for: equipment? needed personnel? training? travel? etc.		

Software Planning Phase (cont.)	RISK	ACTION
Schedule: Is the schedule reasonable considering needed personnel, training, and equipment? Does the system-level schedule accommodate software lifecycle? Can needed equipment be made available in time?		
Has all the slack/contingency time on the critical path been used up?		
Are software metrics kept and reported regularly? Weekly? Monthly?		
Are deviations to the development plan being tracked? Trended? Are the trends reported in a manner to allow timely and appropriate software and project management decisions?		
Will new development techniques be used?		
Will a new or different development environment be used?		
Is this a new technology?		
Will simulators need to be designed and built? Is there time and resources allocated for this?		
Is there a schedule that covers development of both ground and flight software? Is it reasonable, does it match reality? Is it being followed? Are changes tracked and the reasons for the changes well understood?		
Do the schedules for ground and flight software match with what is needed for test and delivery?		
Are there separate schedules for flight and ground? Are different people in charge of them? Are they coordinated by some method?		
Will test software need to be designed and developed? Are there time and resources allocated for this?		
Distributed development environment: Will this be a distributed development (different groups or individuals working on parts of the project in different locations e.g. out of state)? Are there proper facilities and management structure to support distributed development?		
Inter/Intra group management: Are interfaces with other developers, suppliers, users, management, and the customer understood and documented? Is there a known way to resolve differences between these groups (i.e., conflict resolution/ who has ultimate authority, who is willing to make a decision)?		

Software Planning Phase (cont.)	**RISK**	**ACTION**
Management Planning: Is management experienced at managing this size and/or type of team? (Is there an experienced project manager?) Is management familiar with the technology being used (e.g., Formal Methods, OOA/OOD and C++)? Is there a well-constructed software management plan that outlines procedures, deliverables, risk, lifecycle, budget, etc. Is it reasonable, does it match reality? Is it being followed?		
Does software lifecycle approach & timeframe meet needs of overall project; does it have a chance of being close to what is needed?		
Has time been allotted for safety analysis and input?		
Has time been allocated for reliability analysis (e.g., Failure Modes and Effects Analysis (FMEA), Critical Items List (CIL), Fault Tolerance Analysis) input?		
Has time been allocated for software (s/w) quality analysis input and auditing?		
Have software development standards & processes been chosen?		
Have software documentation standards been chosen?		
Has Software Product Assurance given input on all standards, procedures, guidelines, and processes?		
Is funding likely to change from originally projected? Is there a plan in place to handle possible funding changes? Prioritization of requirements? Phasing of requirements delivery?		
Is there a procedure/process for handling changes in requirements? Is it sufficient?		
Examine detailed technical considerations such as: Can the bus bandwidth support projected data packet transfers? Are system requirements defined for loss of power? Is the system reaction to loss of power to the computers known or planned for? Have UPS (Uninterruptable Power Supplies) been planned for critical components?		

Software Requirements Phase	**RISK**	**ACTION**
Software schedule: Is there an adequate software schedule in place? Is it being followed? Are changes to schedule being tracked? Are changes to the schedule made according to a planned process? As events change the schedule, is the decision process for updating the schedule also examined? That is, question if there is something wrong in the process or program that needs to change in order to either make schedule or affect the schedule-updating process? Has the overall schedule been chosen to meet the needs of true software development for this project or has the software schedule merely been worked backwards from a systems NEED date with no consideration for implementation of recommended software development process needs?		
Has all the slack/contingency time on the critical path been used up?		
Are software metrics kept and reported regularly? Weekly? Monthly?		
Are deviations to the development plan being tracked? Trended? Are the trends reported in a manner to allow timely and appropriate software and project management decisions?		
Are parent documents baselined before child documents are reviewed? Is there a process in place for assessing the impact of changes to parent documents on child documents? Is there a process in place for assessing the impact of changes to parent documents from changes within child documents?		
Are review/inspection activities and schedules well defined and coordinated with sufficient lead time for reviewers to review material prior to reviews/inspections?		
Is there a process for closing out all TBDs (to be determined) before their uncertainty can adversely affect the progress of the project?		
Have all the software-related requirements from the systems-level requirements been flowed down? Have the system level and software level standards been chosen? Have the requirements from these standards been flowed down from the system level? Have guidelines, etc., been established?		

Software Requirements Phase (cont.)	RISK	ACTION
Has the project planned how to handle changing requirements? Compartmentalized design? Are procedures/change boards in place for accepting/rejecting proposed changes Are procedures in place for dealing with schedule impacts due to changes? Is the project following these procedures? Is there good communication with the principle investigators/customer? Have requirements been prioritized? Is this prioritization tracked, reviewed, and periodically updated? Is there a clear understanding of what is really necessary for this project?		
Have there been changes/reductions in personnel since first estimates?		
Are there sufficient trained software personnel? Does all the knowledge for any aspect of project reside in just one individual?		
Is there a software testing/verification plan?		
Is the software management plan being followed? Does it need to be adjusted?		
Is the software development environment chosen and in place?		
Does work contracted out have sufficient controls and detail to assure quality, schedule, and meeting of requirements?		
Is a Software Configuration Management (SCM) Plan in place and working?		
Are backups of SCM system/database planned and carried out on a regular basis?		
Are inspections or peer reviews scheduled and taking place?		
Software Quality/Product Assurance (SQA or SPA): Is SPA working with development to incorporate safety, reliability and QA requirements? Is s/w development working with SPA to help establish software processes? Does SPA have a software-auditing process and plan in place?		
Are there good lines of communication established and working between software project groups?		

Software Requirements Phase (cont.)	RISK	ACTION
Are good lines of communication established and working with groups outside software development? Are there written agreements on how to communicate? Are they followed? Are they supported by management and systems group? Are there good interface documents detailing what is expected? Did all the concerned parties have a chance to review and agree to them?		
Have resources been re-evaluated (equipment, personnel, training, etc.)? Are they still sufficient? If not, are steps being taken to adjust project schedule, budget, deliverables, etc. (more personnel, re-prioritization and reduction of requirements, order new equipment, follow previously established mitigation plan, etc.)?		
Are COTS being used? How are COTS maintained? Who owns and who updates them? Is the product affected by changes to COTS? Will new releases of one or more COTS be maintained/supported? Are COTS releases coordinated with the developed software maintenance and releases? Do COTS meet the necessary delivery schedule? Do personnel have a good understanding of how to use/integrate COTS into final product? If the COTS incorporated into the system meet only a subset of requirements of the overall requirements (that is, the COTS software does not completely fulfill the system requirements), have the integration task and time been correctly estimated for merging the COTS with any in-house or contracted software that is needed to complete the requirements? Can this integration task be estimated? Will custom software need to be written to either get different COTS to interact correctly or to interact with the rest of the system as built or planned?		
Is a new technology/methodology being incorporated into software development? Analysis? Design? Implementation? (e.g., Formal Methods. Object Oriented Requirements Analysis, etc.) Has the impact on schedule, budget, training, personnel, current processes been assessed and weighed? Is there process change management in place?		

Software Requirements Phase (cont.)	RISK	ACTION
Is a new technology being considered for the system? Has the impact on schedule, budget, training, personnel, current processes been assessed and weighed? Is there process change management in place?		
Is the project planning to do prototyping of unknown/uncertain areas		

to find out if there are additional requirements, equipment, and/or design criteria that may not be able to be met.		

Software Design Phase	RISK	ACTION
Is the software management plan being followed? Does it need to be updated?		
Is the requirements flow-down well understood?		
Are standards and guidelines sufficient to produce clear, consistent design and code?		
Will there be, has there been, a major loss of personnel (or loss of critical personnel)?		
Is communication between systems and other groups (avionics, fluids, operations, ground software, testing, QA, etc.) and software working well in both directions?		
Requirements: Have they been baselined & are they configuration managed? Is it known who is in charge of them? Is there a clear, traced, managed way to implement changes to the requirements? (i.e., is there a mechanism for inputting new requirements, or for altering old requirements, in place and working)? Is there sufficient communication between those creating & maintaining requirements and those designing to them? Is there a traceability matrix between requirements and design? Does that traceability matrix show the link from requirements to design and then to the appropriate test procedures?		
Has System Safety assessed software? Does any software involved hazard reports? Does software have the s/w subsystem hazard analysis? Do software personnel know how to address safety-critical functions, how to design to mitigate safety risk? Are there fault detection, isolation, and recovery (FDIR) techniques designed for critical software functions?		
Has software reliability been designed for? What level of fault tolerance has been built in to various portions /functions of software?		
Is there a need to create simulators to test software? Were these simulators planned for in the schedule? Are there sufficient resources to create, verify and run them? How heavily does software completion rely on simulators? How valid/accurate (close to the flight unit) are the simulators?		

Software Design Phase (cont.)	RISK	ACTION
Are simulators kept up-to-date with changing flight H/W?		
How heavily does hardware completion rely on simulators?		
Is firmware and/or any other software developed outside the software flight group ? Is it being integrated? Is it being kept current based on changes to requirements & design? Is it configuration managed?		
Does work contracted out have sufficient controls and detail to assure quality, schedule, and meeting of requirements?		
Will design interfaces match in-house or other contracted work?		
Is a software configuration management plan in place and working?		
Are backups of SCM system/database planned and carried out on a regular basis?		
Are Inspections and/or peer reviews scheduled and taking place?		
Software Quality/Product Assurance (SQA or SPA): Is SPA working with development to incorporate safety, reliability, and QA requirements into design? Does SPA have a software-auditing process and plan in place? Have they been using it?		
Are parent documents baselined before child documents are reviewed? Is there a process in place for assessing the impact of changes to parent documents on child documents? Is there a process in place for assessing the impact of changes to parent documents from changes within child documents?		
Are review/inspection activities and schedules well defined and coordinated with sufficient lead time for reviewers to review material prior to reviews/inspections?		
Has all the slack/contingency time on the critical path been used up?		
Are software metrics kept and reported regularly? Weekly? Monthly?		
Are deviations to the development plan being tracked? Trended? Are the trends reported in a manner to allow timely and appropriate software and project management decisions?		

Software Implementation Phase	RISK	ACTION
Coding and unit test		
Is the software management plan still being used? Is it up-to-date?		
Are there coding standards?		
Are they being used?		
Are software development folders (SDFs) being used to capture design and implementation ideas as well as unit test procedures & results?		
Are code walk-throughs and/or inspections being used? Are they effective as implemented?		
Is SQA/SPA auditing development processes and SDFs?		
Is the design well understood and documented?		
Are requirements being flowed down through design properly?		
Is the schedule being maintained? Have impacts been accounted for (technical, resources, etc.)? Is it still reasonable?		
Has all the slack/contingency time on the critical path been used up?		
Are software metrics kept and reported regularly? Weekly? Monthly?		
Are deviations to the development plan being tracked? Trended? Are the trends reported in a manner to allow timely and appropriate software and project management decisions?		
Have any coding requirements for safety-critical code been established? If so, are they being used?		
Does the chosen development environment meet flight standards/needs?		
Has System Safety assessed software (subsystem safety analysis)? Has software reviewed this safety assessment? Has software had input to this safety assessment? Do software personnel known how to address safety critical functions? Is software working with systems to find the best solution to any hazards?		
Has FDIR (fault detection, isolation, and recovery) and/or fault tolerance been left up to implementers (i.e., no hard requirements and/or no design for these)?		
Is there a known recourse/procedure for design changes? Is it understood? Is it used? Does it take into account changes to parent documents? Does it take into account subsequent changes to child documents?		

Software Implementation Phase (cont.)	**RISK**	**ACTION**
Coding and unit test (cont.)		
Is there a known recourse/procedure for requirements changes? Is it understood ? Is it used? Is it adequate; does it need to be altered? Does it take into account changes to parent documents? Does it take into account subsequent changes to child documents?		
Is there development level Software Configuration Management (SCM) (for tracking unbaselined changes and progress)? Is it being used by all developers, regularly? Are backups performed automatically on a regular basis?		
Is there formal SCM and baselining of requirements and design changes?		
Are the design documents baselined?		
Are the requirements baselined?		
Have test procedures been written and approved? Are they of sufficient detail? Will these tests be used for acceptance testing of the system? Are these procedures under SCM? Are they baselined?		
Do some software requirements need to be tested at the systems level for complete verification? Are these documented? Do the systems-level test procedures adequately cover these? Does the requirements/verification matrix indicate which requirements are tested at the systems level?		
For subsystem-level testing: Has software been officially accepted by the subsystems (sign-off, baselined)? Are software testing facilities maintained for any regression testing?		
Are unit testing procedures and results maintained via SCM?		
Is there auto-generated code?		
Is unit testing planned for auto-generated code? Are there procedures for testing unit level auto-generated code?		
Are implementation personnel familiar with the development environment, language, and tools? Sufficiently trained coders (e.g., understand OOA, OOD, C++, Formal Methods, etc., whatever is needed)? Sufficient level of expertise (not first or second time ever done, not just trained)?		

Software Implementation Phase (cont.)	RISK	ACTION
Coding and unit test (cont.)		
Are coders sufficiently familiar with project function/design?		
Do coders have ready access to someone with sufficient expertise and whose time is available for participation in code walk-throughs or inspections and for technical questions?		
Is there sufficient equipment?		
Are there build procedures? Are they documented? Are they under SCM? Are they being followed?		
Are there burn procedures for any PROMS? ROMS? EPROMS? Are they documented? Are they under SCM? Are they being followed? Do they include a method for clearing PROMs (if applicable) and checking them for defects prior to burning? Does the procedure include a method to determine and recording the checksum(s)?		
Are test plans complete? Is further testing needed? Unit level testing? CSCI level testing? Integration testing CSCIs? System-level testing?		
Is the test/requirements matrix up to date?		

Software Implementation Phase (cont.)	**RISK**	**ACTION**
Integration and Systems Testing		
Are review activities and schedules well defined and coordinated?		
Is there a sufficient number of experienced test personnel? Who are experienced on similar projects? Who are experienced with this project? Who are experienced with test equipment, set-up, simulators, hardware? Who are experienced with development environment?		
Is the software test plan being followed? Does it need to be modified? Does it include COTS? Does it include auto-generated code?		
Are there well-written, comprehensive test procedures? Are they up to date? Do they indicate the pass/fail criteria? Do they indicate level of regression testing?		
Are test reports written at the time of the tests?		
Are test reports witnessed and signed off by SPA?		
Is the test/requirements matrix up to date?		
Is there a known recourse/procedure for testing procedure changes? (i.e., is there an Software Configuration Management Process that covers the test procedures?) Is it understood? Is it used? Does it take into account possible changes to parent documents of the test plan or other parent documents? Does it take into account subsequent changes to child documents? Does it take into account regression testing?		
Is there a known recourse/procedure for requirements changes? Is it understood? Is it used? Is it adequate, does it need to be altered? Does it take into account changes to parent documents (e.g., systems requirements)? Does it take into account subsequent changes to child documents (e.g., design and testing documents)?		
Is there Software Configuration Management (SCM) (for tracking baselined changes and progress)? Is it being used? Are backups performed automatically on a regular basis?		

Software Implementation Phase (cont.)	RISK	ACTION
Integration and Systems Testing (cont.)		
Is there formal SCM and baselining of requirements and design changes?		
Are the design documents formally baselined and in SCM?		
Are the software requirements formally baselined?		
Have test procedures been written and approved? Are they of sufficient detail? Do they exist for unit test? Do they exist for CSCI level testing Do they exist for CSCI integration-level testing? Do they exist for software system-level testing? Will these tests be used for acceptance testing to the system? Are these procedures in SCM? Are they baselined?		
Do some software requirements need to be tested at the systems level for complete verification? Are these requirements verification procedures documented? Where are they documented? In software test procedures? In systems test procedures? Do the systems-level test procedures adequately cover these? Does the requirements/verification matrix indicate which requirements are tested at the systems level?		
For system-level testing: Has software been officially accepted by systems (sign-off, baselined)? Are software testing facilities maintained for any regression testing?		
Is firmware ready and tested? Is it baselined and in SCM?		
Are there separate test personnel that have not been designers or coders scheduled to perform the tests? Do they need training? Is time allowed for their unfamiliarity with the system?		
On the flip side, are testers too familiar with software? Will they have a tendency to brush over problems or fix problems without going through proper channels/procedures?		
Have requirements/design/code personnel been moved to other tasks and are no longer available to support testing or error correction?		
Are test pass/fail criteria known and understood?		

Software Implementation Phase (cont.)	**RISK**	**ACTION**
Integration and Systems Testing (cont.)		
Is regression testing planned for? Is there time in the schedule for it? Have estimates been made at each test point of the amount of regression testing necessary to cover fixes if test fails? (e.g., certain failures require complete (end-to-end) re-testing, others may require only re-testing of that test point.)		
Is ground software (or other related software) available for testing or for use in testing flight s/w?		
Has testing of COTS at the software system level been adequately covered and documented? Are there test procedures specifically for proving integration of COTS? Does the requirements to test matrix indicate where COTS is involved?		
Has testing of COTS at the system level been adequately covered and documented?		
Is there good configuration management in place? Is it used? Is there version control? Is error/failure tracking in place? Are PRACA (Problem Report and Corrective Action) and/or s/w change records created? Are problem/change records tracked to closure? Is error correction written into each new release of a module (in code comments, in file header, in SCM version description)? Are incorporated PRACAs listed in the build release version descriptions?		
Will a tight schedule cause: Dropping some tests? Incomplete regression testing? Dropping some fixes? Insufficient time to address major (or minor) design and/or requirements changes? No end-to-end testing? Are these issues being addressed? Who makes these decisions? The change control board? How are they recorded? Does the version description document (VDD) indicate true state of delivered software?		

Software Implementation Phase (cont.)	RISK	ACTION
Integration and Systems Testing (cont.)		
Has all the slack/contingency time on the critical path been used up?		
Are software metrics kept and reported regularly? Weekly? Monthly?		
Are deviations to the development plan being tracked? Trended? Are the trends reported in a manner to allow timely and appropriate software and project management decisions?		

Acceptance Testing and Release	RISK	ACTION
Has pre-ship review already taken place?		
Is actual flight equipment available for software testing? Do the logbook and test procedures record actual flight hardware used for testing?		
Are pass/fail criteria established and followed?		
Is a regression testing procedure documented and known? Is it used?		
Is the procedure to handle PRACAs (Problem Report and Corrective Action) at the acceptance level documented? Is there a change review board in place? Has there been configuration management of changes? Is the PRACA/SPCR (S/W Problem and Change Request) log maintained with status?		
Is systems-level testing adequate to insure software requirements or some software-level testing done separately and documented?		
Is appropriate personnel witness and sign-off testing? SPA or QA involved?		
Are all parts of the architecture verified on the ground prior to flight?		
Does a complete VDD (Version Description Document) exist? In the VDD, are: All delivered software release versions listed? All COTS and their versions listed? All hardware versions appropriate for this release noted? SCM release description(s) provided? Build procedures given? Burn procedures given? Installation procedures provided? List of all incorporated (closed) problem reports and change requests included? List of all outstanding problem reports and change requests included? List of any known bugs and the work-arounds provided? Changes since last formal release indicated? List of all documentation that applies to this release, and its correct version, provided? If there are known discrepancies to hardware, documentation, etc. are these listed and discussed in the VDD?		
Is there clean customer hand-off: Up to date documentation? User/Operations Manual? Code Configuration Managed? All PRACAs & SPCRs closed?		

Acceptance Testing and Release (cont.)	RISK	ACTION
Is there good configuration management wrap-up: Is there a method for future updates/changes in place? Proper off-site storage of data, software and documentation? What happens to SCM and data when project is over?		

APPENDIX C: RELIABILITY DESIGN CHECKLIST

Example taken from:

Reliability (R) and Maintainability (M)

Design Checklist

NAVSEA S0300-AC-MMA-010-R&M

October 1977

Obtainable from:

Naval Publications and Forms Center
5801 Tabor Ave
Philadelphia, Pennsylvania 19120

Attn: Code F01G

PRODUCTION FOLLOW ON

R/M PROGRAM ELEMENTS	TYPE OF CONTRACT: NEW DEVELOPMENT			TYPE OF CONTRACT: MODIFIED DEVELOPMENT		
	A	B	C	A	B	C
PROGRAM PLAN	X	X	X	X	X	X
ORGANIZATION	X	X	X	X	X	X
SUBCONTRACTOR & SUPPLIER CONTROL	X			X		
PROGRAM REVIEW						
R ANALYSIS						
MODEL	X			X		
THERMAL ANALYSIS	X	X		X	X	
ALLOCATION	X			X		
PREDICTION						
SIMILARITY			X			X
AVERAGE STRESS		X			X	
DETAILED STRESS	X			X		
PART CONTROL	X	X		X	X	
FM&EA/FAULT TREE	X	X		X	X	
CRITICAL ITEM CONTROL	X	X		X	X	
STORAGE EFFECTS	X			X		
DESIGN REVIEW	X	X		X	X	

NOTE: See next page for explanation of A, B, and C, above.

R&M LEVELS

LEVEL A

- HIGH LEVEL OF SAFETY
- CRITICAL SYSTEM
- DOWNTIME CRITICAL, MAINTENANCE DIFFICULT AND EXPENSIVE

LEVEL B

- SAFETY FACTOR IN DESIGN
- MODERATELY CRITICAL SYSTEM
- MAINTENANCE MODERATELY DIFFICULT AND EXPENSIVE

LEVEL C

- SAFETY OF MINIMUM CONCERN
- LOW SYSTEM CRITICALITY
- DOWNTIME NOT CRITICAL

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
21	Management			
(a)	Does contractor have a permanent in-house R staff?			
(b)	Is staff composed of experienced R engineers?			
(c)	Does program R engineer report directly to program manager?			
(d)	Does R group have the facility/authority to interface directly with other engineering groups:			
	(1) Design?			
	(2) Systems engineering?			
	(3) Quality Control?			
	(4) Integrated Logistics support?			
	(5) Procurement?			
	(6) Test and Evaluation?			
(e)	Is R group representative(s) member(s) of design review team?			
(f)	Does R group review all drawings and specifications for adequacy of R requirements?			
(g)	Does R program engineer have sign-off authority on all drawings and specifications?			
(h)	Does R engineer/group review Purchase Orders and Purchase specifications to assure all parts and subassemblies are procured with adequate R requirements?			
(i)	Does R group have membership and a voice in decisions for the following:			
	(1) Material Review Board?			
	(2) Failure Review Board?			
	(3) Engineering Change Review Board?			
(j)	Is R group represented on surveys and quality audits of potential subcontractors?			
(k)	Is R group represented at subcontractor design reviews and meetings where R is a topic of discussion?			
(l)	Does an R group member(s) monitor/witness subcontractor R tests?			
(m)	Does R group contain experts in the fields of components/failure analyses?			

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
22	Design for R			
	THERMAL REQUIREMENTS:			
(a)	Have detailed thermal analysis been performed to determine component/module ambient operating temperature?	___	___	
(b)	Has a unit similar to final configuration (e.g., brassboard, preproduction unit, etc.), been instrumented to develop a thermal mapping of the design?	___	___	
(c)	Have anemometer probes been used to measure coolant air flow patterns?	___	___	
(d)	Are equipment internal cooling considerations sufficient to limit internal temperature rises to 20°C maximum?	___	___	
(e)	Are high power dissipation components (e.g., large power resistors, diodes, transformers, etc.) heat sinked?	___	___	
(f)	Where chilled water or chilled air is used for cooling have hermetically sealed components been selected due to possible moisture condensation?	___	___	
(g)	Where chilled water or chilled air is used for cooling are components shielded or otherwise protected from moisture condensation?	___	___	
(h)	Where chilled water or chilled air is used for cooling has consideration been given to removal of condensation to avoid accumulation of moisture and possible fungus growth or corrosion within the equipment?	___	___	
(i)	Are all printed circuit boards conformally coated?	___	___	
(j)	Have circuit performance tests been conducted at high and low temperature extremes to assure circuit stability over the required operating temperature range?	___	___	
(k)	Do heat conducting surfaces make good contact (no air gaps) and have low thermal resistances?	___	___	
(l)	Do surface coatings and paints provide good conduction, convection and radiation coefficients for heat transfer?	___	___	
(m)	Do adhesives where used for fastening components to PCB's or chassis have good thermal conductive properties?	___	___	
(n)	Do potting, encapsulation and conformal coating materials where used have good thermal conducting properties?	___	___	
(o)	Have differences in thermal expansion of interfacing materials been taken into account?	___	___	
(p)	Are high power dissipation components mounted directly to the chasis for better heat sinking rather than encapsulated or thermally insulated?	___	___	
(q)	Is thermal contact area between components and heat sinks kept to a maximum?	___	___	
(r)	Are components sensitive to heat located away from heat flow paths, power supplies and other high power dissipation components?	___	___	
(s)	Are air gaps or thermal insulation provided where necessary to avoid heat flow to temperature sensitive components?	___	___	
(t)	Are temperature overload devices, alarms used to prevent damage due to loss of cooling apparatus?	___	___	
(u)	Do inlet temperature ducts have filters to prevent accumulation of dirt on assemblies which would result in reduction of heat transfer?	___	___	
(v)	Do components mounted on PCB's have adequate lead lengths and are the leads formed to relieve lead stresses during thermal expansion and contraction?	___	___	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Re
	VIBRATION/SHOCK/STRUCTURAL REQUIREMENTS:			
(w)	Has analysis been performed to determine resonant frequencies to be experienced in the equipment environment?	___	___	
(x)	Have detailed vibration/shock/structural analyses been performed to validate structural integrity of the design?	___	___	
(y)	Have critical/unique assemblies been instrumented with accelerometers and tested to verify design adequacy with respect to vibration and shock transmissibility factors?	___	___	
(z)	Have structural mountings been designed to resonate away from resonant frequencies and their harmonics?	___	___	
(aa)	Have damping considerations been applied to subassemblies and components mounting where natural frequencies are close to expected environmental frequencies?	___	___	
(bb)	Are large components (over 1/2 oz.) being clamped or tied down to the chassis or printed circuit boards to prevent high stresses or fatigue failure of electrical leads?	___	___	
(cc)	Heavy components are mounted near corners of the chassis near mounting points for direct structural support rather than between supports?	___	___	
(dd)	Centers of gravity of heavy components are kept low close to the plane of the mounts?	___	___	
(ee)	Are cables/harnesses clamped close to terminal connections to avoid resonances and prevent stress and failure at the point of connection?	___	___	
(ff)	Do cables/wires have sufficient slack to prevent stresses during thermal changes and mechanical vibration/shock?	___	___	
(gg)	Stranded wire is used when cabling might be susceptible to fatigue failure?	___	___	
(hh)	Components and subassemblies have adequate sway space to avoid collision during vibration and shock?	___	___	
(ii)	Welding (not spot welding) and/or riveting is used for permanently attached structural members rather than nuts and bolts?	___	___	
(jj)	All component leads have minimum bend radii to avoid overstressing?	___	___	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
	MISCELLANEOUS REQUIREMENTS:			
(kk)	Has consideration been given to avoid the use of dissimilar metals?	___	___	
(ll)	Have the PCB's been designed for the following considerations:			
	(1) PCB material is compatible with storage and operating temperature (plus operating temperature rises) with respect to:			
	(1) PCB material?	___	___	
	(2) Metal cladding/bonding strengths?	___	___	
	(3) Board warping?	___	___	
	(2) PCB resistivity is sufficiently high to meet circuit leakage current requirements even under high humidity?	___	___	
	(3) PCB arc resistance is sufficiently high where high voltages are present?	___	___	
	(4) PCB dielectric constraint is sufficiently low to prevent building up of unwanted capacitances?	___	___	
	(5) PCB flexural strengths (function of board material and dimensions) is sufficient to meet structural and vibration requirements?	___	___	
	(6) PCB conductors width is sufficient to handle maximum current flow without harmful heat generation or resistance drop?	___	___	
	(7) PCB's have plated through holes to aid in soldering of lead electrical connections?	___	___	
	(8) PCB conductor spacings have a minimum spacing based upon voltage between conductor (e.g., .025" per 150 volts peak)?	___	___	
	(9) PCB conductor paths are spaced and designed to keep capacitance between conductors to a minimum?	___	___	
	(10) Are PCB's conformally coated?	___	___	
(mm)	Where encapsulation, embedding and potting used, does the material have:			
	(1) Good thermal conductivity for heat transfer?	___	___	
	(2) Good electrical isolation/dielectric ?	___	___	
	(3) Provide dampening for shock and vibration?	___	___	
	(4) Thermal expansion coefficients which match those of items encapsulated?	___	___	
	(5) Will not crack or shatter under vibration and mechanical and thermal shock?	___	___	
	(6) Has good chemical stability under anticipated use environments?	___	___	
(nn)	Have worst case analyses or statistical variation of parameters been conducted to determine required component electrical tolerances considering:			
	(1) Manufacturing tolerances?	___	___	
	(2) Tolerances due to temperature changes?	___	___	
	(3) Tolerances due to aging?	___	___	
	(4) Tolerances due to humidity?	___	___	
	(5) Tolerances due to high frequency or other operating constraints?	___	___	
(oo)	Has redundancy been considered for critical functions where practical?	___	___	
(pp)	Where redundancy is used, has considerations been given to avoid common mode failure situations which could disable all redundant circuits?	___	___	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remai
(qq)	Has design practices been applied to obtain RFI suppression such as:			
	(1) Use alternating current non-commutating machinery rather than direct current machinery when feasible?			
	(2) Provide optimum interference suppression with two twisted wires in a common shield whenever wire pairs can be used?			
	(3) Use short wires in preference to long wires?			
	(4) Filter power lines to remove harmonics and other types of inherent interference?			
	(5) Mount filters as close to interference sources as possible without altering the effectiveness of the filter?			
	(6) Use bonding techniques to insure that good electrical contact is made between chassis, conduit, shielding, connectors, structural and housing metal parts?			
	(7) Remove non-conducting coatings from bolts, nuts, and tapped holes?			
	(8) Internally shield invididual sections of equipment which are either highly susceptible to interference or which generate interference. For example, the r-f input stages and local oscillators should be shielded individually?			
	(9) Use a bandwidth consistent with the minimum possible value for the received signal. This often improves the signal-to-noise ratio?			
	(10) Use direct current filament sources where practicable?			
	(11) Ground center tap of filament transformer secondary winding to reduce hum?			
	(12) Avoid the use of gaseous lighting devices in the vicinity of sensitive wiring or electronic equipment?			
	(13) Do not cable noisy and clean leads together?			
	(14) Never route cables near known interference sources?			
	(15) Do not use shields or metal structures for return current paths?			
	(16) Avoid the use of corrosion preventive compounds with high insulating qualities at bond joints?			
(rr)	Have considerations been given to preclude damage due to:			
	(1) Installation?			
	(2) Handling?			
	(3) Transportation?			
	(4) Storage?			
	(5) Shelf Life?			
	(6) Packaging?			
	(7) Maintenance environment?			
	(8) Other environments:			
	(a) Humidity?			
	(b) Fungus?			
	(c) Sand and dust?			
	(d) Salt atmosphere?			
(ss)	Has reliability been considered as a factor in all tradeoff studies affecting equipment reliability?			

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
23	Parts Program			
(a)	Does contractor have a Parts Control Board (PCB) to promote proper selection and application of parts used in the design?	___	___	
(b)	Has contractor established and maintained an up-to-date Preferred Parts List (PPL) to be used by designers?	___	___	
(c)	Has contractor established derating guidelines for derating of electrical/electronic parts electrical stresses?	___	___	
(d)	Do derating guidelines correspond to specification requirements?	___	___	
(e)	Has contractor developed part application guidelines for proper selection of part types for circuit use?	___	___	
(f)	Are military grade parts used in the design?	___	___	
(g)	Are non-standard parts used only when a military equivalent part cannot be obtained?	___	___	
(h)	Where non-standard parts are used do they have adequate qualification/test data and a history of high reliability?	___	___	
(i)	Where non-standard parts are used are they procured via specification control drawing which specifies:			
	(1) Reliability requirements?	___	___	
	(2) Environmental requirements?	___	___	
	(3) Test requirements?	___	___	
(j)	Has contractor submitted non-standard part data for approval per applicable specification (e.g., MIL-STD-749/965)?	___	___	
(k)	Do parts used in the design meet the environmental requirements to which they will be subjected during use with respect to:			
	(1) Operating temperature (plus worst case internal case temperature rises)?	___	___	
	(2) Non-operating/storage temperature?	___	___	
	(3) Humidity?	___	___	
	(4) Vibration?	___	___	
	(5) Shock?	___	___	
(l)	Have parts been reviewed for proper application, have part stresses been calculated ( ) or measured ( ) and do they meet:			
	(1) Derating guidelines?	___	___	
	(2) Application guidelines?	___	___	
(m)	Are established reliability (ER) components and JAN semiconductors and microcircuit devices used in the design?	___	___	
(n)	Where ER components are used, is the most representative level of all ER components used:			
	(1) L?	___	___	
	(2) M?	___	___	
	(3) P?	___	___	
	(4) R?	___	___	
	(5) S?	___	___	
	(6) T?	___	___	
(o)	Where JAN semiconductors (MIL-S-19500) are used, the most representative level of all such devices used are:			
	(1) JAN?	___	___	
	(2) JANTX?	___	___	
	(3) JANTXV?	___	___	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
(p)	Where JAN microcircuits (MIL-M-38510) or high quality microcircuits are used the most representative level of all such devices used are:			
	(1) MIL-M-38510 Class S ?	___	___	
	(2) MIL-M-38510 Class B ?	___	___	
	(3) MIL-M-38510 Class C ?	___	___	
	(4) MIL-STD-883 Class S ?	___	___	
	(5) MIL-STD-883 Class B ?	___	___	
	(6) MIL-STD-883 Class C ?	___	___	
	(7) Vendor equivalent to _______?	___	___	
(q)	Do parts meet the interchangeability requirements of MIL-STD-454 Requirement 7?	___	___	
(r)	Do all parts selected meet the life requirements of the equipment?	___	___	
(s)	Are handling requirements specified for critical and delicate parts susceptible to damage, degradation, contamination from shock, vibration, static electric discharge, uncleanliness, etc.?	___	___	
(t)	Are assembly and cleaning procedures specified to prevent damage to components during assembly on PCB's, chassis, etc.?	___	___	
(u)	Have dominant failure modes of a particular part type been considered in the selection of that part?	___	___	
(v)	Are fixed rather than variable components (such as resistors, capacitors, inductors, etc.) used in the design wherever possible?	___	___	
(w)	Are all relays, motors, dynamotors, rotary power converters, etc. suppressed so as not to produce excessive spikes or transients during operation?	___	___	
(x)	Are all semiconductor devices silicon rather than Germanium?	___	___	
(y)	Plastic coated and/or encapsulated semiconductor devices are not used?	___	___	
(z)	Do all microcircuits have hermetically sealed ceramic cases rather than plastic cases?	___	___	
(aa)	Do all microcircuits used have at least two potential suppliers?	___	___	
(bb)	Do all unused gates of a digital microcircuit have inputs grounded?	___	___	
(cc)	Are the number of expandable gates limited to no more than 75% of allowable number of expandables?	___	___	
(dd)	Where humidity is not controlled are hermetically sealed resistors, capacitors, relays, etc., used?	___	___	
(ee)	Are all power supplies designed and manufactured in-house?	___	___	
(ff)	Are parts, even MIL-M-38510, JANTX, Established Reliability (ER) parts screened at incoming inspection:			
	(1) 100%?	___	___	
	(2) Sampling plan per ____________________?	___	___	
	(3) Environmentally ____________________?	___	___	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
24	Developmental Test Program			
(a)	Is contractor conducting a developmental test program?	___	___	
(b)	Does developmental test program include:			
	(1) All critical assemblies?	___	___	
	(2) Each assembly with a unique form factor?	___	___	
	(3) Critical non-standard parts?	___	___	
(c)	Does developmental testing include environmental testing at or above the levels specified for qualification:			
	(1) High and low temperature?	___	___	
	(2) Vibration?	___	___	
	(3) Shock?	___	___	
	(4) Humidity?	___	___	
(d)	Are performance requirements checked over required operating temperature levels?	___	___	
(e)	Are life tests or reliability tests of critical components/subassemblies being or have they been conducted?	___	___	
(f)	Is "Step Stress" testing being performed on subassemblies, etc., to determine design margins?	___	___	
(g)	Is developmental test program monitored by the reliability group or does the reliability group provide inputs to developmental testing?	___	___	
(h)	Are failure data and maintenance data collected during developmental testing for determining need for reliability improvement?	___	___	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
25	Reliability Analyses			
(a)	Have the following reliability analyses been performed:			
	(1) Reliability Mathematical Models?	___	___	
	(2) Reliability Apportionments?	___	___	
	(3) Reliability Predictions?	___	___	
	(4) Failure Modes and Effects Analyses?	___	___	
	(5) Criticality Analyses?	___	___	
	(6) Circuit Analysis (nominal and worst cases)?	___	___	
	(7) Thermal Analysis?	___	___	
	(8) Sneak Circuit Analysis?	___	___	
(b)	Do predictions meet apportioned values?	___	___	
(c)	Do predictions meet numerical reliability specification requirements?	___	___	
(d)	Have the results of the predictions been used to increase equipment reliability by:			
	(1) Reduction of circuit complexity?	___	___	
	(2) Reduction of ambient temperature conditions?	___	___	
	(3) Reduction of internal temperature rises?	___	___	
	(4) Reduction of part stresses by further derating?	___	___	
	(5) Increase of part quality levels?	___	___	
	(6) Addition of redundancy?	___	___	
(e)	Has a numerical approach for Criticality Analysis been used?	___	___	
(f)	Does the numerical criticality analysis consider:			
	(1) Frequency of failure?	___	___	
	(2) Degree of effect on system performance?	___	___	
	(3) Difficulty to diagnose and/or repair?	___	___	
	(4) Personnel or equipment safety?	___	___	
(g)	Have all critical modes of system failure been identified?	___	___	
(h)	Have critical items been ranked as to criticality?	___	___	
(k)	Has the use of limited life items been kept to a minimum?	___	___	
(l)	Have the analyses considered the effects of storage, transportation and handling on failure modes, effects and failure rates?	___	___	
(m)	Has the use of circuit analysis provided a stable, design over the worst case conditions?	___	___	
(n)	Has protective circuitry been utilized in the equipment design?	___	___	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
26	Burn-in Program			
(a)	Does the contractor impose burn-in at:			
	(1) Component level?	___	___	
	(2) Subassembly/module level?	___	___	
	(3) Equipment/system level?	___	___	
(b)	Is burn-in performed under:			
	(1) Temperature (elevated)?	___	___	
	(2) Temperature cycling?	___	___	
	(3) Vibration?	___	___	
(c)	Are lengths of burn-in adequate for each level?	___	___	
(d)	Do spares receive same burn-in as modules/subassembly level?	___	___	
(e)	Do all equipments/systems receive the same amount of burn-in?	___	___	
(f)	Does contractor have a failure free burn-in requirement prior to acceptance of the equipment?	___	___	
(g)	Is random vibration performed?	___	___	
	(1) Equipment level? ________			
	(2) "g" level? ________			
	(3) Frequency range? ________			
	(4) Time duration? ________			

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remar
27	Failure Reporting Analysis and Corrective Action (FRACA) Program			
(a)	Has contractor implemented a FRACA program?	___	___	
(b)	Does FRACA program cover failures during:			
	(1) Source inspection at subcontractor's plant?	___	___	
	(2) Incoming inspection?	___	___	
	(3) In-process inspection?	___	___	
	(4) Development tests?	___	___	
	(5) Subassembly/module test?	___	___	
	(6) Equipment integration and checkout?	___	___	
	(7) Equipment burn-in?	___	___	
	(8) Equipment formal tests:			
	(a) Acceptance tests?	___	___	
	(b) Environmental/qualification tests?	___	___	
	(c) Reliability/Maintainability tests?	___	___	
(c)	Does contractor have in-house facilities for performing detailed failure analysis?	___	___	
(d)	Is failure analysis conducted for all failures?	___	___	
(e)	Are failures summarized by part number and failure type to determine trends and patterns?	___	___	
(f)	Has contractor established thresholds (percent defective or failure rate) for determining need for corrective action?	___	___	
(g)	Does failure report form contain the necessary information with regards to:			
	(1) Identification of failed part subassembly, assembly, etc.?	___	___	
	(2) Elapsed time meters (for failure at equipment level)?	___	___	
	(3) Failure symptoms?	___	___	
(g)	(4) Effect of failure on system/equipment?	___	___	
	(5) Test and environmental conditions at time of failure?	___	___	
	(6) Suspected cause of failure?	___	___	
(h)	Is the same type of FRACA program imposed upon subcontractors of critical subassemblies?	___	___	
(i)	Are subcontractor failure reports included in contractor failure summaries?	___	___	
(j)	Are all failure reports, analyses and corrective actions reviewed by the reliability group?	___	___	
(k)	Are failure trends monitored by the reliability group?	___	___	
(l)	Are corrective actions involving design changes tested in the equipment for an adequate period of time prior to their formalization?	___	___	
(m)	Are corrective action investigations reopened upon a recurrence of the same type of failure?	___	___	
(n)	Are proposed corrective actions referred to the Procuring Activity for concurrence?	___	___	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
28	Reliability Demonstration Test Planning			
(a)	Will test simulate operating profile that will be seen aboard ship?	___	___	
(b)	Will all modes of equipment operation be tested?	___	___	
(c)	Is definition of failure in accordance with contract specification requirements?	___	___	
(d)	Are relevant and non-relevant failure definitions adequately defined?	___	___	
(e)	Will test be performed under environmental levels specified by the contract specifications?	___	___	
(f)	Will burn-in to be performed on reliability test units be no more or no less than that specified for production units?	___	___	
(g)	Non-operating and equipment standby time will be discounted from applicable test time for validating reliability, true?	___	___	
(h)	No Preventive Maintenance other than that contained in technical manuals and approved by the Navy will be performed during the test, true?	___	___	
(i)	Performance checks capable of checking the complete equipment failure rate, performed no less frequently than daily have been defined for the test, true?	___	___	
(j)	Test will be performed per agreed schedule, true?	___	___	
(k)	Procuring Activity will be notified of the exact test date at least 30 days prior to the test, true?	___	___	
(l)	All interfaces are simulated or stimulated?	___	___	
(m)	All interfaces are real?	___	___	
(n)	If interfaces are real, is GFE required?	___	___	
(o)	If GFE is required, has a request been made to obtain GFE?	___	___	
(p)	Is test DD 1423 documentation on schedule?	___	___	

1. Is design simple? Minimum number of parts?
2. Is it designed into a unified overall system rather than as an accumulation of parts, etc.?
3. Is the item compatible with system in which it is used?
4. Is the item properly integrated and installed in the system?
5. Are there adequate indicators to verify critical functions?
6. Has reliability for spares and repair parts been considered?
7. Are reliability requirements established for critical items? For each part?
8. Is there specific reliability design criteria for each item?
9. Have reliability tests been established?
10. Are standard high-reliability parts being used?
11. Are unreliable parts identified?
12. Has the failure rate for each part or part class been established?
13. Have parts been selected to meet reliability requirements?
14. Have below-state-of-the-art parts or problems been identified?
15. Has shelf life of parts been determined?
16. Have limited-life parts been identified, and inspection, and replacement requirements specified?
17. Have critical parts which required special procurement, testing, and handling been identified?
18. Have stress analyses been accomplished?
19. Have derating factors been used in the application of parts?
20. Have safety factors and safety margin been used in the application of parts?
21. Are circuit safety margins ample?
22. Have standard and proven circuits been utilized?
23. Has the need for the selection of parts (matching) been eliminated?
24. Have circuit studies been made considering variability and degradation of electrical parameters of parts?
25. Have solid-state devices been used where practicable?

FIGURE 7.11.4-2: TYPICAL QUESTIONS CHECKLIST FOR THE DESIGN REVIEW (SHEET 1 of

26. Is the reliability or MTBF of the item based on actual application of the parts?

    a. Comparison made with reliability goal?

    b. Provision for necessary design adjustments?

27. Are the best available methods for reducing the adverse effects of operational environments on critical parts being utilized?

28. Has provision been made for the use of electronic failure prediction techniques, including marginal testing?

29. Is there provision for improvements to eliminate design inadquacies observed in tests?

30. Have normal modes of failure and the magnitude of each mode for each item or critical part been identified?

31. In the application of failure rates of items to reliability equations, have the following effects been considered?

    a. External effects on the next higher level which the item is located.

    b. Internal effects on the item.

    c. Common effects, or direct effect of one item on another item, because of mechanical or electro-mechanical linkage.

32. Has redundancy been provided where needed to meet specified reliability?

33. Has failure mode and effects analyses been adequately covered by design?

34. Have the risks associated with critical item failures been identified? Accepted? Has design action been taken?

35. Does the design account for early failure, useful life and wear-out?

ιE 7.11.4-2: TYPICAL QUESTIONS CHECKLIST FOR THE DESIGN REVIEW (SHEET 2 of 2)