PROGRAM RISK ID

Radical Risk Identification for Meeting Program Objectives

Laurie Wiggins
CEO
Sysenex Inc.
What is the Problem?

Program Overruns (and performance problems too)

In March 2014, the GAO reported that the 72 major defense programs they reviewed that have reached the systems development stage were averaging 23 months delay in delivering initial capabilities.¹

MADRID, Jan 1 (Reuters) - Work on the massive Panama Canal extension project may be suspended after a clash between the builders and the Panamanian authorities about $1.6 billion in cost overruns, according to a statement from the building consortium on Wednesday. The cost overruns on the $3.2 billion canal extension, one of the world's largest construction contracts….²

‘Management errors in Airbus’ A400M cargo plane program allowed huge cost overruns’³ It was delayed a total of four years and has gone 6.2 billion euros (US$8.3bn) over budget - a 30 percent overrun.⁴

---

² Reuters | January 1, 2014
³ http://blog.seattlepi.com/aerospace/2010/01/20/audit-finds-eads-can-pay-for-a400m-cost-overruns/ January 2010
No One Wants to Get Bitten
As highly experienced professionals, let’s talk about your experiences and observations of projects (or seeing projects) that failed, were seriously delayed, or had major cost over runs.

• What were the issues that arose that caused these things to happen?
• In theory, could these issues been predicted early?
• If so, how would this have changed things for your clients and your firm?
A Typical Risk Management Process

1. Risk Identification
   - Identify Risks
   - Risk events and their relationships are defined

2. Risk Impact Assessment
   - Assess Probability & Consequence
   - Probabilities and consequences of risk events are assessed

3. Risk Prioritization Analysis
   - Assess Risk Criticality
   - Decision-analytic rules applied to rank-order identified risk events from "most to least" critical

4. Risk Mitigation Planning, Implementation, and Progress Monitoring
   - Risk Mitigation
   - Risk events assessed as medium or high criticality might go into risk mitigation planning and implementation; low critical risks might be tracked/monitored on a watch list.

Consequences may include cost, schedule, technical performance impacts, as well as capability or functionality impacts.

Source: MITRE
Why Do Risk Management?

A. My management requires it
B. Customer or regulatory requirement
C. Standard Process
D. To save money and time
E. To kill bad ideas
F. To cover yourself
G. Other
Why Do Risk Management?

Because the customer requires it (89%) or

To comply with existing regulations (65%)

Per our survey
Why Is RM Required by Customer/Regulation?

RM = Risk Management
Risk Management Today

Problems found late in development cost 500-1000 times more to address

Effectiveness Costs

Source: INCOSE
75% of companies surveyed have a RM process and use it.

51% of them have suffered risk related loss or failure.

Per our survey.
Why Isn’t the Risk Management Process More Effective?

The Piecemeal Approach to Risk Management
- the Gulf Oil Spill

The Subjectivity of Risk Management

Denial, Fear and Embarrassment About Risk
Let’s focus on risk identification
Risk Identification Today

We’ve been doing it the same way for 50+ years
Current RI methods are ad hoc

- Personal experience/lessons learned: 83.3%
- Consult SMEs/Program Personnel: 71.4%
- Brainstorming: 66.6%
- Failure Analyses: 54.7%
- Consult Stakeholders: 50.0%
- PRA: 40.5%

Current RI methods are non-comprehensive
- Doesn’t cover all program areas

Not much RI help is available
- A Sysenex/George Mason University study revealed 50+ commercially available risk tools – none of which identify risk
The Downside of Undiscovered Risks

- Will occur at the worst possible time and in the worst possible way
  - Cost and schedule overruns
  - Performance impacts

- Loss of reputation – yours, your company

  “It takes 20 years to build a reputation and 5 minutes to ruin it ….”
  
  Warren Buffett

- Potential program failure

- Job losses – yours, others
Risk Identification Analysis

- Over 500 programs, their risks and outcomes were analyzed
- The same risks kept coming up, over and over
- Although risk specifics vary by program, the \textit{underlying causes are the same}
- 218 common risks identified
- Risk weighting based on risk frequency, severity
Risk Identification Analysis

Components of a Thorough Risk Evaluation

Program complexity
- Greater complexity = greater risk
- Simple, average, moderate, intermediate and high

Objective risk evaluation – two parts
- The risk line item
- Program status of the risk at this time
Risk Identification Analysis

218 Risks in six areas

- Operational
- Technical
- Managerial
- Organizational
- Enterprise
- External

Current Risk ID
Enterprise Risk Management
Risk Identification Analysis

Risk Area Breakouts - Selected Risks

**Technical**
- Requirements Definition
- Interface Definition and Control
- Common Mode/Cascading Failures
- Quality
- Safety
- Logistics Supportability
- Technology Maturity
- Failure Analysis
- Models and Simulations
- Data Quality
- Software Module Maturity
- Software Integration Maturity
- Experience Required to Implement HW Module
- HS Methodology and Process Maturity
- Change Management Process
- Productivity
- Testing Planning
- COTS/GOTS/Reuse Experience

**Organizational**
- Organizational Management Processes
- Organizational Interest in Personnel Motivation
- Organizational Culture
- Organizational Experience
- Organizational Business/Mission Benefit

**Enterprise**
- Enterprise Reputation
- Enterprise Experience
- Enterprise Management Processes
- Enterprise Security Processes
- Enterprise Contingency Planning

**Management**
- Management Experience
- Resources and Commitment
- Overall Program Staffing
- Personnel Experience
- Turnover Rate
- Personnel Morale
- Subcontractor Management
- Supplier Management

**Operational**
- System Operational Problems
- Obsolescence Management Process
- Personnel Training and Experience
- Human Error
- Near Miss Consideration
- User Acceptance
- User Satisfaction
- System Availability
- System Failure Contingencies

**External**
- Funding
- Regulatory
- Legal
- Labor Market
- Customer Experience
- Customer Interaction

---

19
Changes the RM Paradigm

A web-based software tool

For One Program – trending through time

Across Many Programs - compare risk levels across programs
**Anatomy of a PRID Risk**

**EXR6 - Funding**

Select the risk level that most accurately describes your program.

**Risk Levels**

1. Funding is completed for the program life cycle. There is no known threat to funding.
2. Required funding is committed for the program.Allocations are completed for next year.
3. Funding is allocated for out-years. There is some threat to continued funding at the required levels.
4. There is no funding allocated for the out-years. There is a high threat to continued funding.
5. Required funding is not committed for the program, and there is an extreme threat to present funding.

N/A. This risk is not applicable to the program

**User Notes (Optional)**
Enter any relevant comments to explain the choice that you selected above.
Anatomy of a PRID Risk

TR1 - Requirements Definition

Select the risk level that most accurately describes your program.

Risk Levels

1. System and user requirements are fully defined and formally agreed to by all stakeholders.

2. System and user requirements are partially defined; the remainder are to be defined in the short term and formally agreed to by all stakeholders.

3. System and user requirements are not defined, forcing the developer to make assumptions. Assumptions are informally agreed to by the stakeholders or users. Potential for definition of requirements in the short term exists.

4. System and user requirements are not defined, forcing the developer to make assumptions. Assumptions are informally agreed to by the stakeholders or users. There is no potential for definition of requirements for the long term.

5. System and user requirements are not defined, forcing the developer to make assumptions. There is no potential for definition of requirements for the long term.

N/A. This risk is not applicable to the program.
Anatomy of a PRID Risk

MR11 - Management Experience

Select the risk level that most accurately describes your program.

Risk Levels

1. Similar work has been successfully completed more than once, and most of the senior management experience is still available.

2. Similar work has been successfully completed more than once, and some of the senior management experience is still available.

3. Similar programs have been successfully completed once, and some of the senior management experience is still available.

4. Similar programs have been successfully completed once, but most senior management experience is no longer available.

5. No similar programs have been successfully completed under existing senior management.

N/A. This risk is not applicable to the program
PRID Risk Organization

PRID Risk Hierarchy:

Risk Area
  ↓
Risk Category
  ↓
Individual Risk

Technical Risks
  ↓
System Design
  ↓
Design Maturity

PRID Example:
Demonstration and Reporting
• Trending allows measurement of risk mitigation efforts through subsequent analyses
  - changes in risk level = changes in scores

• Portfolio Management
  - using a common standard makes common problems visible
  - which programs are in the most trouble? Enables better resource allocation
Now that you have these risks, what’s next?

PRID tool reports become the input for other risk tools
  • commercial, homegrown
Program Risk ID
Who should we talk to in your organization? Referrals?

www.programriskid.com