Risk Management and Beyond

2010 NDIA Systems Engineering Conference
San Diego, California

Presented by
Al Florence

Co

Agenda

- ➡ • ***Tutorial Objectives***
  - Introduction
  - Reasons for Risk/Issue Management
  - Opportunities
  - Risk Management
  - Issue Management
  - Risk/Issue Avoidance
  - Risk/Issue Opportunities
  - Questions/Discussion
  - References
  - Contact Information

MITRE *AI Florence*

Tutorial Objectives

- Emphasize the importance of identifying and managing program risks and issues

- Clarify the difference between risks and issues

- Present Risk/Issue Avoidance
  - The elimination of the sources of high risk by replacing them with a lower-risk alternatives
  - The establishment of sound technical, programmatic and management practices and activities early and their execution throughout the entire life cycle to reduce risks and issues

- Present opportunities associated with risks/issues
  - When perusing new opportunities risks and issues are encountered
    - By taking calculated risks organizations may realize future opportunities
  - Opportunities to improve program and project performance may surface while resolving risks and issues

Where Are We

- Tutorial Objectives
- **➡ *Introduction***
    - *Definitions*
- Reasons for Risk/Issue Management
- Opportunities
- Risk Management
- Issue Management
- Risk/Issue Avoidance
- Risk/Issue Opportunities
- Opportunity/Risk/Issue/Opportunity Scenario
- Questions/ Discussion
- References
- Contact Information

MITRE *AI Florence*

Introduction

Definitions

- Risks (IEEE Std 1540-2004; Standard for Software Life Cycle Processes)
  - Program and project risks are the likelihood of an event, hazard, threat, or situation occurring and its undesirable consequences
- Risk (Project Management Body of Knowledge PMBOK)
  - An uncertain even or condition that, if it occurs, has a positive or negative effect on project's objectives
- Issues (QATAR National Project Management)
  - An issue is something currently happening that is having a negative impact on the project and requires resolution for the project to proceed successful
- Issues
  - An issue can be associated with a risk if the risk is realized; has occurred
- Opportunity (The American Heritage Dictionary)
  - A favorable or advantageous combination of circumstances
  - A chance for progress or advancement
- Opportunity (PMBOK)
  - A condition or situation favorable to the project, a positive set of circumstances, a positive set of events, a risk that will have a positive impact on project objectives, or a possibility for positive chances
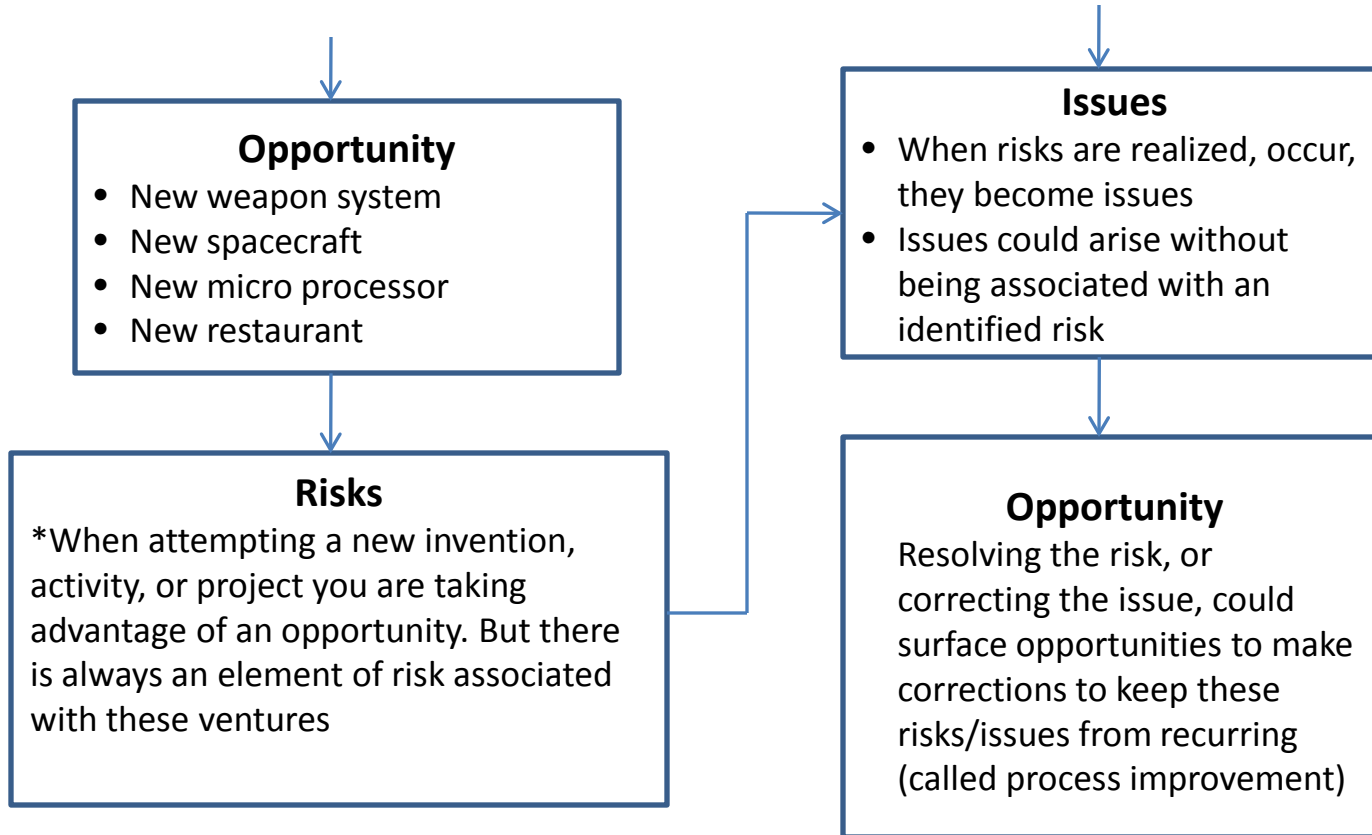
Introduction
Definitions

- Risk Response
  - The process of developing options and actions to enhance opportunities and reduce threats to project objectives   PMBOK
  - Includes Mitigation and Contingencies
  - Includes acceptance of the risk or issue consequence

- Mitigation
  - Risk mitigation implies an elimination or reduction in the probability of risk occurrence   PMBOK

- Contingency
  - Issue contingency implies an elimination or reduction of the impact of issues or alternative actions taken

MITRE *AI Florence*

Introduction

- We will start with Opportunities and end with Opportunities
    - Opportunity
    - Risk
    - Issue
    - Opportunity

Introduction

Opportunity
- New weapon system
- New spacecraft
- New micro processor
- New restaurant

Issues
- When risks are realized, occur, they become issues
- Issues could arise without being associated with an identified risk

Risks
*When attempting a new invention, activity, or project you are taking advantage of an opportunity. But there is always an element of risk associated with these ventures

Opportunity
Resolving the risk, or correcting the issue, could surface opportunities to make corrections to keep these risks/issues from recurring (called process improvement)

*Managing Risks, Methods for Software Systems Development; Dr. Elaine M. Hall, SEI Series in Software Engineering

Where Are We

- Tutorial Objectives
- Introduction
➡ - ***Reasons for Risk/Issue Management***
- Opportunities
- Risk Management
- Issue Management
- Risk/Issue Avoidance
- Risk/Issue Opportunities
- Questions/Discussion
- References
- Contact Information

MITRE *AI Florence*

Reasons for Risk/Issue Management

- When developing, delivering, and acquiring systems and products
  - developers and acquirers face many challenges

- Challenges can exist with many items and activities:
  - Cost
  - Schedule
  - Technical
  - Management
  - Programmatic
  - Process
  - Performance
  - Others?

Reasons for Risk/Issue Management

- Consequences may be numerous if challenges are not mitigated
  - Cost overruns
  - Late deliveries
  - Technically inadequate
  - Programmatic difficulties
  - Irate management
  - Irate customer
  - Canceled project
  - Loss of market share
  - Missed opportunities
  - Others?

MITRE *AI Florence*

Reasons for Risk/Issue Management

- There are solutions for an organization to help mitigate these challenges
  - Proper program/project management
  - Proper program/project planning
  - Program/project monitoring and control
  - Adequate budgets
  - Adequate schedules
  - Proper requirements development and management
  - Contract tracking and oversight
  - Product evaluation
  - Performance management
  - *Risk/Issue management*
  - Quality assurance
  - Configuration management
  - Independent Verification and Validation (IV&V)
  - Others?

MITRE *AI Florence*

Reasons for Risk/Issue Management

- It is important to recognize risks and issues early and manage them to reduce or eliminate their impact if they occur

- Often organizations neglect risk and issue management or do not provide sufficient attention to them

Compliance with CMMI ®

- Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI)
  - CMMI for Development v1.2
  - CMMI for Acquisition v1.2
  - CMMI for Service v1.2
  - V1.3 release soon for all

All have
Risk Management and
*Issue Management
Process Areas

In order for organizations to be compliant with CMMI they need to establish risk and issue management capabilities

* Issue management is implied in the Project Planning, Project Monitoring and Control, Quality Assurance and Configuration Management

Where Are We

- Tutorial Objectives
- Introduction
- Reasons for Risk/Issue Management
→ - ***Opportunities***
- Risk Management
- Issue Management
- Risk/Issue Avoidance
- Risk/Issue Opportunities
- Questions/ Discussion
- References
- Contact Information

MITRE *AI Florence*

Take Advantage of Opportunities

- Risks are not always undesirable events
  - Taking risks can sometimes be necessary
  - If we are not willing to take calculated risks our advancement in technology and business may be hindered
- We have to be circumspect with the risks we are willing to take
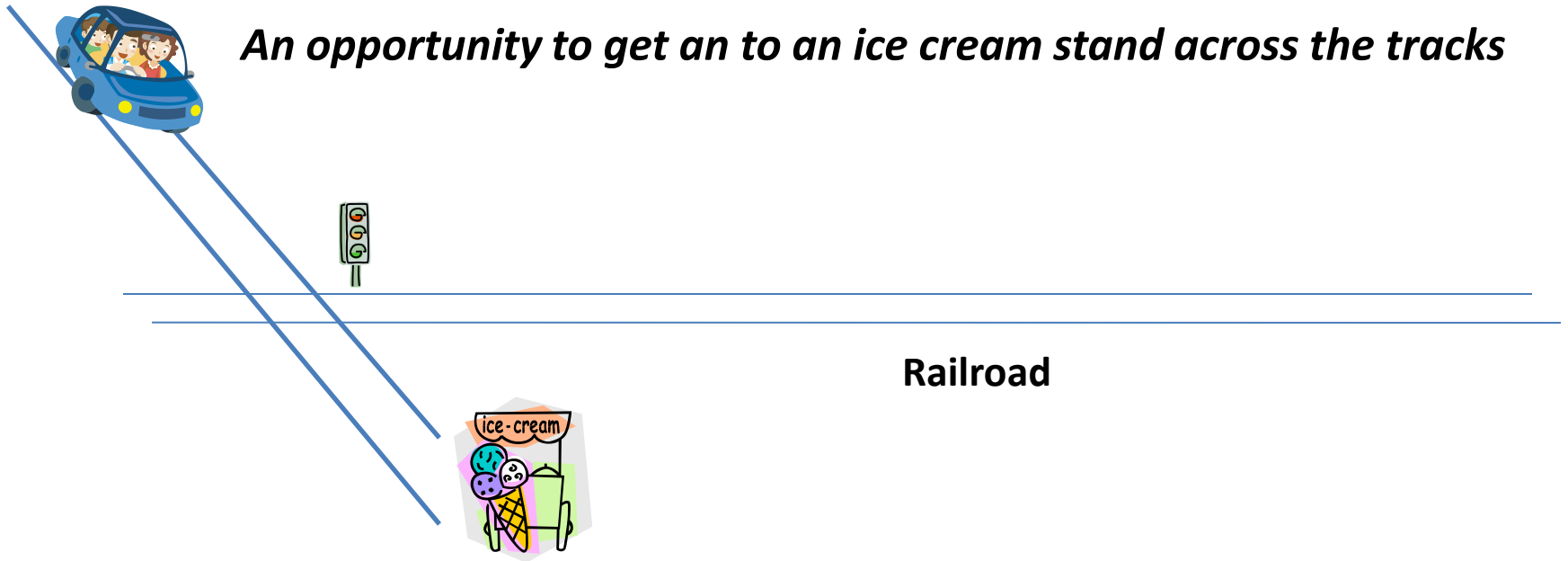 - And *MANAGE* them properly

Take Advantage of Opportunities

Opportunities/Risks

*Running away from risk is a no-win strategy. Unless your organization has been sound asleep for the past 30 years, all the relatively risk-free opportunities have long since been exploited. The remaining high-opportunity areas are rife with risk. It is in these areas and these alone where you need to focus your attention, skills and resources.

*Managing Risks, Methods for Software Systems Development; Dr. Elaine M. Hall,
SEI Series in Software Engineering*

MITRE *AI Florence*

Opportunity

An opportunity to get an to an ice cream stand across the tracks

Railroad

Where Are We

- Tutorial Objectives
- Introduction
- Reasons for Risk/Issue Management
- Opportunities
→ - *Risk Management*
- Issue Management
- Risk/Issue Avoidance
- Risk/Issue Opportunities
- Questions/ Discussion
- References
- Contact Information

MITRE *AI Florence*

Risk Management Process

- Risk Management is an overarching process that encompasses
  - Risk Planning
  - Risk Identification
  - Risk Analysis
  - Risk Response
  - Risk Monitoring and Control

  PMBOK

Risk Management Flow

MITRE *AI Florence*

21
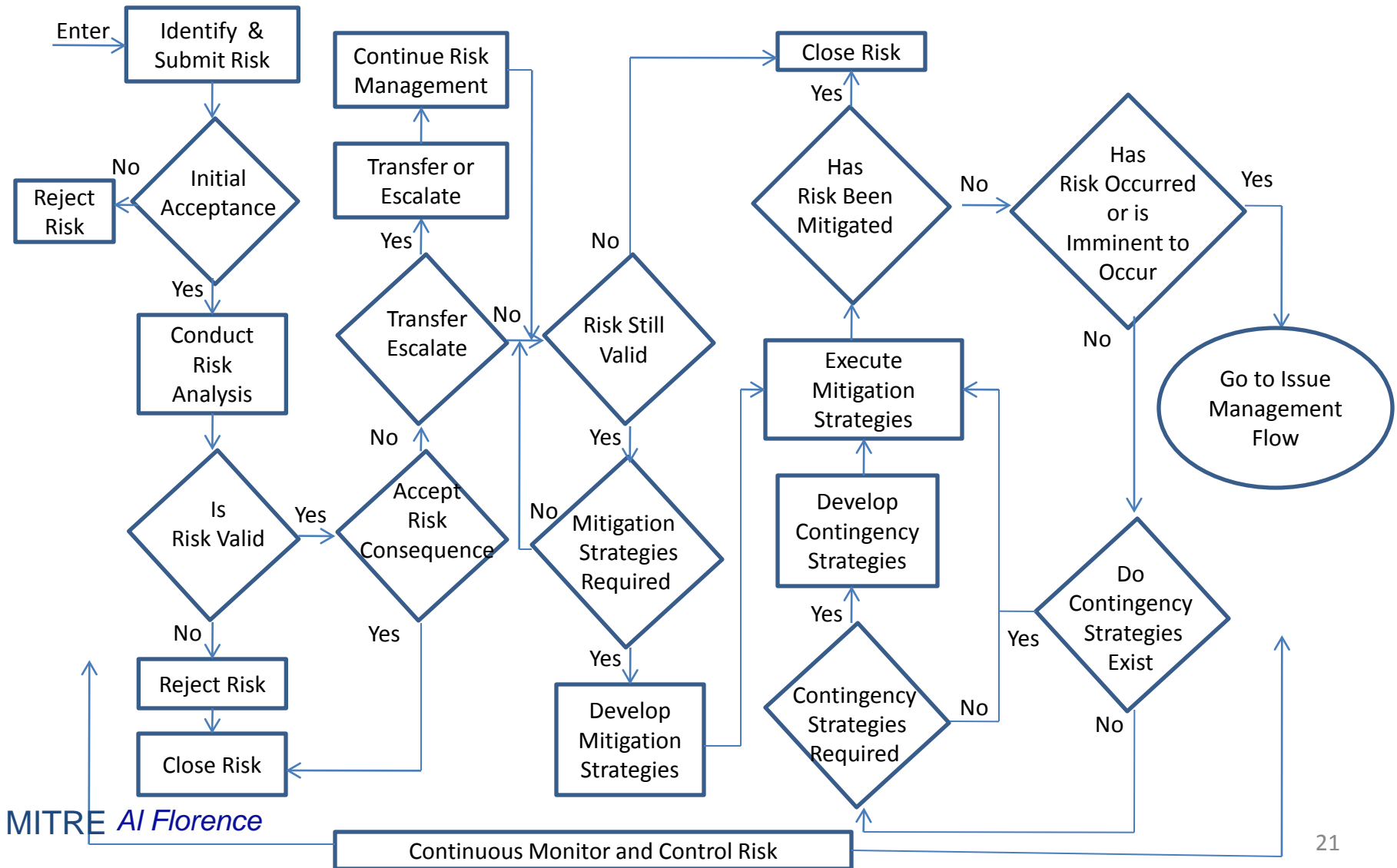
Risk Management Planning

- Risk management planning is the process of deciding how to approach and conduct the risk management activities for a project
- Planning is important to
  - Ensure the level, type and visibility of risk management are commensurate with both the risk and importance of the project to the organization
  - Provide sufficient resources and time for risk management activities
  - Establish an agreed-upon basis for evaluating risks
- Risk planning should be completed early during project planning

PMBOK

Risk Management Team

- The Risk Managment planning activity may assign a Risk Management Team to administer the Risk Management Program
- A Risk Manager may be assigned to manage the Risk Management Team
- A Risk Management Board may be chartered to review, accept, decline, transfer and escalate risks
- Hierarchy Governance Boards may exist for escalation of risks based on thresholds
- Everyone on the program/project is responsible for risk management

> The level of this implementation depends on the size, scope, critically, safety, security, etc. of the application

Risk Management Plan

- Risk management planning needs to be part of project planning

- A risk management plan can be a stand alone plan or part of the project plan

- The risk management plan needs to be tailored to the scope of the application

- The concepts provided in this tutorial can be used to develop the plan

Risk Management Plan Outline

- Introduction
- Project Description
- Risks/Issue/Opportunity Descriptions
- Risk Identification
- Risk Analysis
- Risk Response
  - Risk Acceptance
  - Risk Avoidance
  - Risk Transfer
  - Risk Escalation
  - Risk Mitigation
- Risk Monitor and Control
- Risk Register
- Issue Management
- Issue Contingency
- Risk/Issue Opportunities
- Risk/Issue Training
- Glossary
- References

Risk Management Artifacts

- Risk Management is supported with:
  - Risk Management Policy
  - Risk Management Charter
  - Risk Process Description
  - Risk Management Plan
  - Risk Management Procedures
  - Risk Management Guidelines
  - Risk Management Training

- This presentation will not dwell on these but content of this presentation can support their construction/implementation

MITRE *AI Florence*

Risk Identification

- Risk Identification is the activity that:
  - Identifies potential and current risks
  - Examine elements of the program to identify associated potential root causes of risks
  - Begin their documentation
  - Sets the stage for their successful management
  - Risk identification begins as early as possible in successful programs and continues throughout the life of the program
  - Project and stakeholders from outside and inside the project should be involved in risk identification

MITRE *AI Florence*

Risk Identification

- Risk can be associated with all aspects of a program; e.g.
    - Requirements
    - Threat
    - Security
    - Technology maturity
    - Supplier capability
    - Design
    - Schedule
    - Cost
    - Performance
    - Etc.

Risk Description

- As risks are identified it is important to correctly describe them
- A well-written risk statement contains three main components:
    - Cause – The negative <u>conditions</u> that currently exist relative to the risk
        - Identification of root cause(s) of the risk
        - This provides justification that a risk exists
    - Probability of Occurrence – The <u>likelihood</u> of the occurrence of the risk
        - Within a future time frame
        - Or a future event
    - Consequence – The <u>effect(s)</u>, negative impact(s) to the program(s) in case the risk occurs
        - The consequence should be related to at least cost, schedule, scope and performance
        - Consequence could also result in opportunities that may surface in correcting the problems

Risk Description

- The risk is written in a chain of: Cause: IF; THEN

Example

An Interface Working Group has not been formed and a plan to form one does not exist. **IF** key stakeholders cannot agree on interface protocol by 10/25/2010; **THEN** the schedule for development and delivery will be delayed causing cost overruns.

NOTE: The cause includes assurance that the reason for the risk is valid. I.e., is there a compelling reasons(a root cause) to assume that stakeholders cannot agree on the interface protocol by 04/26/2010? *Not just pie in the sky.*

Risk Description

- Proper risk descriptions helps manage the right risks
  - Risk management is time and resource consuming
  - Managing "non-risks" is not cost effective
- Example
  - A risk may be identified as a risk that component YYY will be provided late
  - Writing this risk as:
    - **IF** component YYY is delivered late; **THEN** …
  - May fail to inspire interest and action
    - The risk is too vague, or
    - There is no clear reason why this is a risk
  - In this case one needs to identify causal conditions that may prevent timely delivery of YYY. *If there are none this is not a risk!*

Risk Description

- The cause may be included in the "IF" statements for some risk**s**

> **IF** scheduled delivery of component YYY continues to slip beyond 10/25/2010; **THEN** system integration will also slip causing the system to incur cost and schedule overruns.

- Cause
  - Written in the IF statement
  - Schedule continues to slip
- Occurrence
  - Schedule delivery slips beyond 04/26/2010
- Consequence
  - Cost and schedule overruns

MITRE *AI Florence*

Risk Description

- Avoid writing the mitigation strategy into the risk description
  - A mitigation strategy is developed after the risk has been approved and analyzed

Examples

> Requirements have always been a problem in passed projects within this organization. **IF** requirements are not reviewed and verified; **THEN** requirement defects will migrate into the design.

- Reviewed and verified are possible mitigation strategies
- Write the risk in a chain of cause, occurrence, consequence

> Requirements have always been a problem in passed projects within this organization. **IF** defective requirements are not discovered and corrected by PDR; **THEN** requirements defects will migrate into the design and implementation causing rework, and cost and schedule impacts.

Risk Description

- Risks must be written in a clear, concise and unambiguous fashion

- Words and phrases that may have confusing and multiple interpretations must be avoided

Ambiguous Words

- Avoid ambiguous words in describing risks, some examples:
    - Adequate
    - Ad hoc
    - All
    - Always
    - Appropriate
    - Clearly
    - Easy
    - Existing
    - Fast
    - Flexible
    - Future
    - If required
    - Immediately
    - Large
    - Light
    - Limited
    - Near real time
    - Periodic
    - Portable
    - Rapid
    - Several
    - Slow
    - Small
    - Sometimes
    - State of the art
    - Sufficient
    - Usable
    - User-friendly
    - Weight
    - When required
    - Others?

From IEEE standards and some preparatory requirements management plans

Also: http://www.ppi-int.com/newsletter/SyEN-017.php#article

MITRE *AI Florence*

Risk Analysis

- The risk is submitted to the Risk Management Board

- The risk is accepted or declined by the Board
  - If declined rational is conveyed to the submitter

- If accepted the Risk Management Board assigns:
  - A Risk Analyst responsible for conducting risk analysis on assigned risks
    - Supported by Subject Matter Experts (SMEs)
  - A Risk Owner responsible for ensuring risks are properly managed throughout their life
  - Risk Analyst and Owner could be one in the same

Risk Analysis Components

- Risks have the following components:
  - A future root cause(s) (yet to happen) which
    - if eliminated or corrected, would prevent a potential consequence from occurring
  - A probability of occurrence (or likelihood)
    - assessed at the present time and updated when necessary of the future root cause occurring
  - The consequence (or effect/impact) of that future occurrence
  - The time horizon during which the consequences will occur if the risk is not mitigated
  - Risk Priorities
    - Mapping of probability of risk occurrence and risk consequence
  - Risk Triggers
    - Specific events or conditions that indicate when to develop and execute mitigation or contingency strategies

.

Risk Analysis

- **Qualitative Risk Analysis**

  - Relative measure of risk or asset value based on ranking or separation into descriptive categories such as low, medium, high; not important, important, very important; or on a scale from 1 to 10.

    BusinessDictionary.com
  - An examination and prioritization of the risks based on their probability of occurring and the impact on the project if they do occur. Qualitative risk analysis guides the risk reaction process.
    pmpbank.googlepages.com/glossary

- **Quantitative Risk Analysis**

  - Incorporates numerical estimates of frequency or probability and consequence. In practice, a sophisticated analysis of risk requires extensive data which are expensive to acquire or often unavailable. Fortunately, few decisions require sophisticated quantification of both frequency and consequences
  - Shortly spoken one might say that "quantitative risk analysis breaks down risks from a high medium low ranking to actual numerical values and probabilities of occurrence" for being able to compute the overall effects
     (comp. CROSSWIND7, p. 423)

Root Causes

- A future root cause is the most basic reason for the presence of a risk
- The cause of the risk has to be isolated and defined
  - Root causes should be initially identified when risks are identified
  - Once initial root cause are identified they may need to be analyzed further to determine the actual deep rooted causes of the risks
  - Root causes are documented and they support:
    - Establishing risk mitigation and contingency strategies
    - Improvement opportunities
- Root causes can also be referred as risk drivers

Root Cause Analysis. An analytical technique used to determine the basic underlying reason that causes a variance or a defect or a risk. A root cause may underlie more than one variance or defect or risk. ((PMBOK® Guide) -- Fourth Edition) Syn: root-cause analysis

Root Causes

- Typical root causes may be associated with:

  - Threat
  - Requirements
  - Technical Baseline
  - Test and Evaluation
  - Modeling and Simulation
  - Technology
  - Logistics

  - Management
  - Schedules
  - External Factors
  - Budget
  - Earned Value Management
  - Production
  - Industrial Capabilities
  - Cost
  - Others?

MITRE *AI Florence*

Root Causes

Background Information

- <u>Threat</u> - The sensitivity of the program to uncertainty in the threat description, the degree to which the program would have to change if the threat's parameters change

- <u>Requirements</u> - The sensitivity of the program to uncertainty in the system requirements

- <u>Technical Baseline</u> - The approved and fixed configuration of a technical item at a specific time in its lifecycle that serves as a reference point for change control

- <u>Test and Evaluation</u> - The adequacy and capability of the test and evaluation program to assess attainment of significant performance specifications and determine whether the system is operationally effective, operationally suitable, and interoperable with the system

MITRE *AI Florence*

Root Causes
Background Information

- <u>Modeling and Simulation</u> - The adequacy and capability of M&S to support all life-cycle phases of a program using verified, validated, and accredited models and simulations

- <u>Technology</u> - The degree to which the technology proposed for the program has demonstrated sufficient maturity to be realistically capable of meeting all of the program's objectives

- <u>Logistics</u> - The ability of the system configuration and associated documentation to achieve the program's logistics objectives based on the system design, maintenance concept, support system design, and availability of support data and resources

MITRE *AI Florence*

Root Causes

Background Information

- Management - The degree to which program plans and strategies exist and are realistic and consistent. The program support team should be qualified and sufficiently staffed to manage the program

- Schedule - The sufficiency of the time allocated for performing the defined tasks

- External Factors - The availability of resources external to the program that are required to support the program such as facilities, resources, personnel, government furnished equipment, etc.

- Budget - The sensitivity of the program to budget variations and reductions and the resultant program turbulence

- Earned Value Management (EVM) - The adequacy of the EVM process and the realism of the integrated baseline for managing the program

Root Causes

Background Information

- Production - The ability of the system configuration to achieve the program's production objectives based on the system design, manufacturing processes chosen, and availability of manufacturing resources

- Industrial Capabilities - The abilities, experience, resources, and knowledge of the contractors to design, develop, manufacture, and support the system

- Cost - The ability of the system to achieve the program's life-cycle cost objectives. This includes the effects of budget and affordability decisions and the effects of inherent errors in the cost

Probability of Occurrence

- Probability of occurrence assessed, at the present time, is the probability of a future root cause occurring

- The chance of a risk occurring is rated on a scale between >0 and 1

- When the probability of occurrence = 1; (100%)
  - The risk has occurred; it then becomes an issue and is managed as an issue

- For most risks, estimating the precise probability of occurrence may be difficult
  - Analysis by SMEs may be necessary, and often using Best Engineering Judgment

Probability Scores

- Probability of occurrence may begin with a qualitative description of probability, which will tie to a numeric range of probability.

Sample Risk Probability Scores

Probability Description	Probability % of Occurrence
Very High (Extremely likely)	≥81% and =100%
High (Probable)	61% – 80%
Medium (Possible)	41% – 60%
Low (Unlikely)	21% – 40%
Very Low (Highly improbable)	>I% – ≤20%

Consequence of Risk Occurrence (Impact)

- Risks are reviewed for the effect that they would have on the project's objectives and other elements of the program

- The level of impact, may be rated from very low (1) to very high (5), and is assessed against at least four categories:

    - Cost
    - Schedule
    - Scope
    - Performance

Consequence of Risk Occurrence

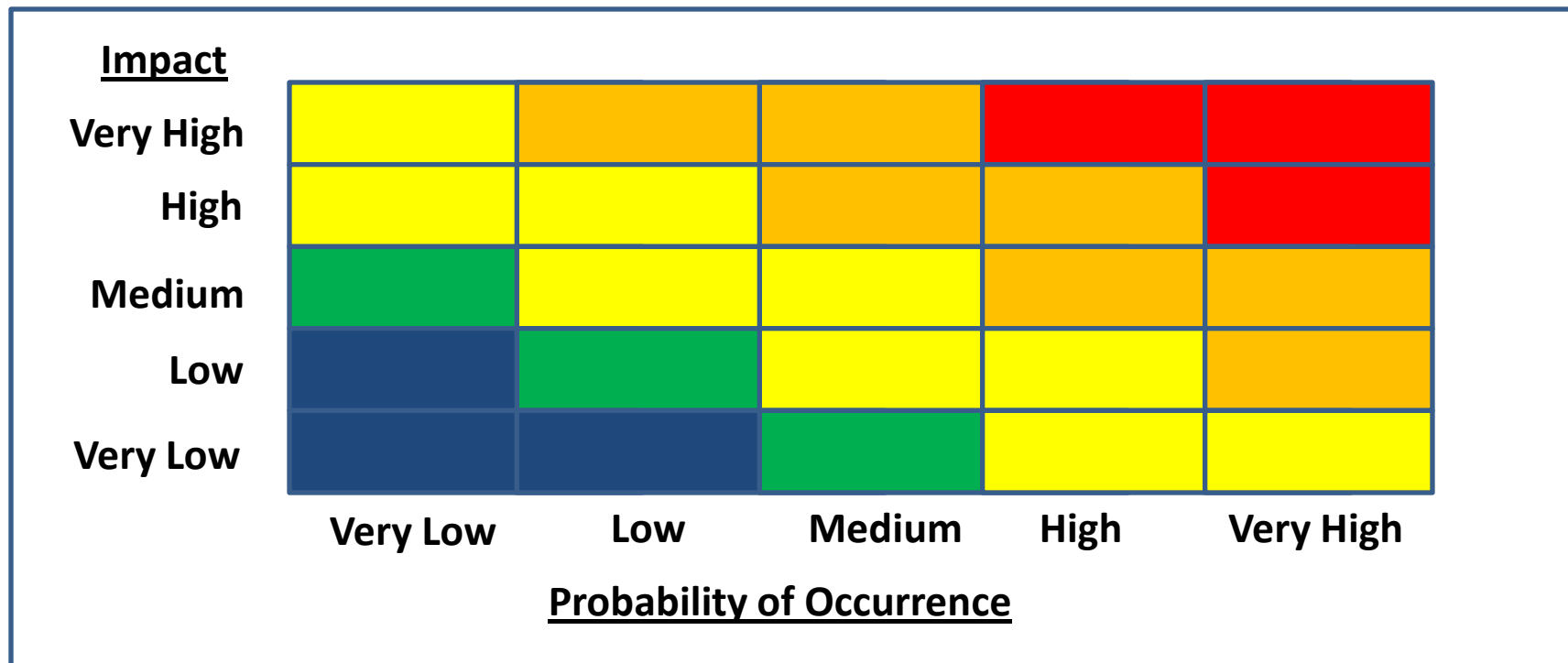| Program/Project Objective	Very Low Minor	Low Moderate	Medium Serious	High Critical	Very High Catastrophic
Cost	Insignificant increase	Increase < 2% of budget baseline	Increase 2–5% of budget baseline	Increase 6–10% of budget baseline	Increase > 10% of budget baseline
Schedule	Insignificant slippage	Slippage < 2% of project baseline schedule	Slippage 2–5% of project baseline schedule	Slippage 6–10% of project baseline schedule	Slippage > 10% of project baseline schedule — OR — Slippage past a milestone mandated by Congress
Scope	Scope decrease barely noticeable	Minor areas of scope affected	Major areas of scope affected	Scope reduction unacceptable to sponsor	Project outcome is effectively useless
Performance	Performance degradation barely noticeable	Performance degradation noticeable, but does not fail acceptance criteria	Performance reduction requires sponsor approval	Performance reduction unacceptable to sponsor	Project outcome is effectively useless

Time Horizon

- There are at least three dates that may be specified for each risk:

  - Near risks are those in which the earliest date of the risk impact is within xx days of the present date

  - Mid risks are those in which the earliest date of risk impact is between xx and zz days from the present date

  - Far risks are those in which the earliest dates of the risk impact are greater than zz days from the present date

  (xx<zz)

- These dates are used as triggers to track when the risk will begin to impact the program and/or when the risk has been overcome by events

Near Risks   Mid Risks   Far Risks

XX   ZZ   Time

MITRE *AI Florence*

Risk Exposure

- Risk exposure. ([ISO/IEC 16085:2006 Systems and software engineering--Life cycle processes--Risk management](#)

  (1) the potential loss presented to an individual, project, or organization by a risk

  (2) a function of the likelihood that the risk will occur and the magnitude of the consequences of its occurrence

- Risk exposure can also be called **Risk Priority**
  - The priority of a risk helps to determine the amount of resources and time that should be dedicated to managing and monitoring the risk
  - Very Low, Low, Medium, High, and Very High priority is assessed by using probability and impact scores
  - The potential timing of a risk event may also be considered when determining risk management actions

Risk Priorities

Impact

	Very Low	Low	Medium	High	Very High
Very High	🟨	🟧	🟧	🟥	🟥
High	🟨	🟨	🟧	🟧	🟥
Medium	🟩	🟨	🟨	🟧	🟧
Low	🟦	🟩	🟨	🟨	🟧
Very Low	🟦	🟦	🟩	🟨	🟨

Probability of Occurrence

🟦 Very Low Priority 🟩 Low Priority 🟨 Medium Priority 🟧 High Priority 🟥 Very High Priority

Risk Priority vs. Mitigation/Contingency

| Very Low Priority	Low Priority	Medium Priority	High Priority	Very High Priority
↓	↓	↓	↓	↓
Risk Watch List	Monitor	Monitor	Monitor	Monitor
		Develop Mitigation Strategy	Develop Contingency Strategy	

Very Low Priority Risks are placed in a Risk Watch List which are periodically monitored.
Other Risks are monitored more aggressively.

Risk Priorities & Time Horizon

The potential timing of a risk event may also be considered when determining risk management actions
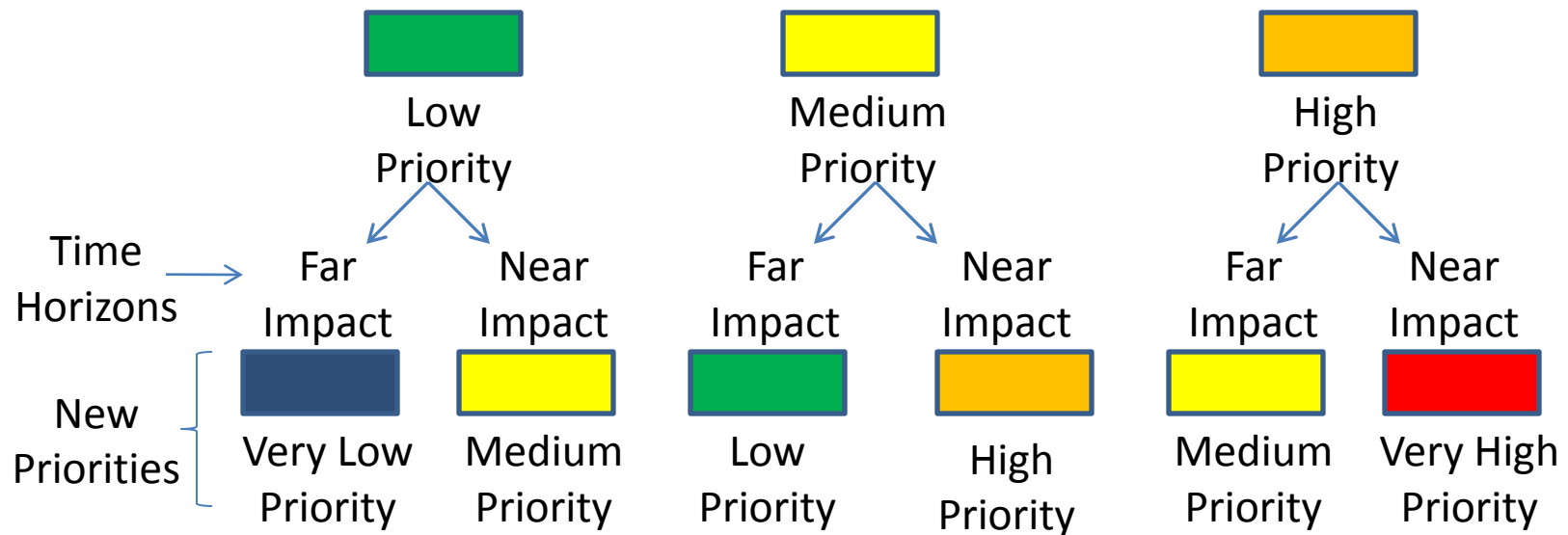
Time Horizons may influence the Risk Priority
(Mid Time Horizon should not influence risk priority change)

Priorities may change over time

Identifying Triggers

- Triggers are specific events or conditions that indicate when to execute mitigation or contingency strategies

- Unless a condition is immediate, a trigger should be defined

- Examples of triggers may include:
  - Cost performance
  - Schedule performance
  - Results of management reviews
  - Occurrence of the risk
    - as a trigger for execution of contingency strategies

Risk Response

- Risk response is the process of developing options and determining actions to enhance opportunities and reduce threats to the project's objectives

- Risk response must be
  - Appropriate to the significance of the risk
  - Cost effective in meeting the challenge
  - Timely and realistic within the project contend
  - Agreed to by all parties involved

PMPOK

Risk Response

- Risk Responses has at least five components
  - Acceptance
  - Avoidance
  - Transfer
  - Escalate
  - Mitigate *(contingencies – for issues)*
- Acceptance – Accept the consequences of the risk occurring
  - Other responses may not be possible
  - Cost to respond may be greater than the benefit
  - May not be possible to prevent the impact if the risk occurs
  - Impact may be negligible
  - Risk may be imminent and should be handled as an issue

Risk Avoidance/Transfer

- Avoidance *(covered later in presentation)*
  - Eliminate the sources of high risk and replace them with a lower-risk alternative
  - Risk avoidance with good management and engineering practices
- Transfer - Shift the responsibility of managing and resolving the risk to another party
  - May be better able to manage the risk
  - May be the proper owner of the risk
  - Transfer could be from one party to another within the same organization
  - Transfer could be to a completely different organization

Risk Escalation

- Escalation - Risks should be managed at the lowest practical level
  - But conditions may arise where a risk should be escalated to higher levels of management or beyond the program/project
  - The next higher organizational (Governance) entity may be able to better to handle the risk/issue
  - Thresholds may exist that determine escalation
    - Cost of impact
    - Schedule effect of Impact
    - Scope of impact
    - Performance effect of impact
    - Time critical
    - Cost critical

Risk Mitigation

- Taking early action to reduce the probability and/or impact of a risk occurring is often more effective that trying to repair the damage after the risk has occurred

- Adapting less complex processes, conducting more tests, or choosing a more stable supplier are examples of mitigation actions

PMBOK

Risk Mitigation

- The following are important guidelines for effective risk mitigation:
  - Prepare detailed mitigation strategies for all medium, high and very high risks
    - With sufficient detail about what is to be done, when, where, and by whom
  - Develop mitigation strategies as early as possible, allowing time to address risks needing special attention or action
    - Helps reduce the chance of having high-priority risks appear at the last moment on the critical path
  - Prepare contingency strategies for all high and very high priority risks and risks imminent to occur

Risk Mitigation
Background Information

- Adaptations of the following strategies can be applied to a range of risks. This list is intended merely as a starting point for thinking about risk mitigation

  - Multiple Development Efforts - Create competing systems in parallel that meet the same scope and performance requirements

  - Alternative Design - Create a backup design option that uses a less risky approach

  - Trade Studies – Conduct studies to arrive at the least risky solution

  - Early Prototyping - Build and test prototypes early in the system development

  - Incremental Development - Design with the intent of upgrading system parts in the future

MITRE *AI Florence*

Risk Mitigation
Background Information

– Technology Maturation Efforts - Normally, technology maturation is used when the desired technology will replace an existing technology that is available for use in the system

– Robust Design - This approach, while it could be more costly, uses advanced design and manufacturing techniques that promote quality through design

– Reviews, Walk-Throughs, and Inspections - These three actions can be used to reduce the probability/likelihood and potential consequences/impacts of risks through timely assessment of actual or planned events

– Design of Experiments - This engineering tool identifies critical design factors that are sensitive, and therefore potentially high-risk, to achieve a particular user requirement

MITRE *AI Florence*

# Risk Mitigation
Background Information

- Open Systems - Carefully selected commercial specifications and standards, which can result in lower risks

- Use of Standard Items/Software Reuse - Use of existing and proven hardware and software, where applicable, can substantially reduce risks

- Use of Mock-Ups - The use of mock-ups, especially man-machine interface mock-ups, can be used to conduct early exploration of design options

- Modeling/Simulation - Modeling and simulation can be used to investigate various design options and system requirement levels

- Key Parameter Control Boards - The practice of establishing a control board for a parameter may be appropriate when a particular feature (such as system weight) is crucial to achieving the overall program requirements

MITRE *AI Florence*

Issue Contingency

- Issue contingencies are developed for high and very high priority risks

- Covered further under issues

Risk

Probability of occurrence 40% – Low
Consequence of occurrence – Very High
Risk Priority – Medium
Mitigation – Hit breaks

Signal Broken
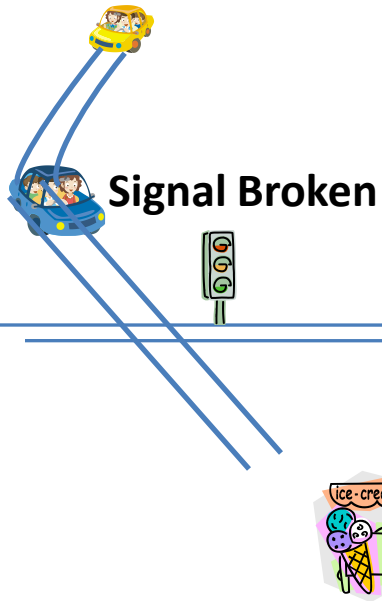
Train approaching 2 mile away going 60 mph

Risk Monitoring and Control

- In order to effectively monitor and control risks a Risk Repository needs to be established
  - Also called a Risk Register
- There are many risk tools that provide repository capabilities:
  - Home developed tools
  - Commercial tools
  - Corporate/agency tools

  Note: Risk register implementation may depend on project size. A month long project might just need a spread sheet table whereas a multi-year, geographically dispersed project may require an internet and SQL-based database tool.

Risk Control

- Risk control involves:
  - Plan and execute actions that reduce the probability/impact of a risk on the project's objectives (i.e., mitigation); and/or
  - Establish a feasible impact control plan for the realization of the risk (i.e., contingency)
  - Control includes the decision to:
    - Close risks
    - Mark risks as occurred
    - Update probability and impacts and other details (conduct additional analysis)

MITRE *AI Florence*

Risk Records

- Risk and Issue records in a risk/issue repository serve several purposes:
  - Reporting and communicating information to others who might be impacted or who might be able to help manage an item
  - Providing risk lists and status for reviews with stakeholders
  - Assisting the risk originator and owner the collection of information about an item
  - Helping risk owners and others to easily access risk and issue information, and manage that information to the benefit of the organization

Risk/Issue Repository

- Suggested contents of repository
  - Category of risk (schedule, cost, technical, management, etc.)
  - Risk Identifier
    - Unique alpha numeric identifier of each risk/issue
  - Risk Name
    - Descriptive name of risk or issue
  - Risk Description
    - Cause
    - Probability of Occurrence - **IF**
    - Consequence - **THEN**

Risk/Issue Repository

- Suggested contents of repository
  - Stage in which the risk exists at time
    - Analysis, Mitigation, Contingency, Issue, Closed
  - Priority
    - Very Low, Low, Medium, High, Very High
  - Impact
    - Very Low, Low, Medium, High, Very High
  - Probability of Occurrence
    - Larger then zero equal to 1 for risks
    - If 1 it becomes an issue
  - Risk Triggers
  - Mitigation Strategies
  - Contingency Strategies
  - Notes

Risk Monitoring

- Risk monitoring involves
  - Tracking individual risks, primarily by reviewing the status of their mitigation strategies, probability, consequence, and other information
  - Risk Monitoring includes:
    - Continuous reassessment of risks
    - Reporting on risks
  - Continuously analysis and status updates in the Risk/Issue Repository
  - Providing evidence to outside governance bodies that the program and its projects have identified sources of uncertainty and possible failure

Risk Monitoring provides data and status for Risk Control activities

Risk Monitoring

- Critical review makes certain that the solution is fixing the root cause wherever possible and prepares the risk owner and project to answer the following questions:
  - What is the expected reduction of probability and impact? Is it documented? Is it a sufficient reduction?
  - Can the option be feasibly implemented and still meet the user's needs?
  - Is time available to develop and implement the option?
  - Is the mitigation strategy affordable in terms of cost and other resources (e.g., use of critical materials, test facilities, etc.)? Does the benefit outweigh the cost?
  - What effect does the option have on the overall program schedule?
  - What effect does the option have on the system's technical scope and performance?

Risk Monitoring

- Risk reports can be in the form of text reports and/or graphs

- The following are examples of reports and metrics that can be reported:

  - Open Risk/Issues by Priority by Month
  - Closed Risks/Issues Current Month
  - Risk/Issue Plans
    - Current and next month
  - Risk/Issue Transfer Current Month
  - Risk/Issue Escalation Current Month
  - Risk/Issue Activity History
  - Risk/Issue for Management Attention

MITRE *AI Florence*
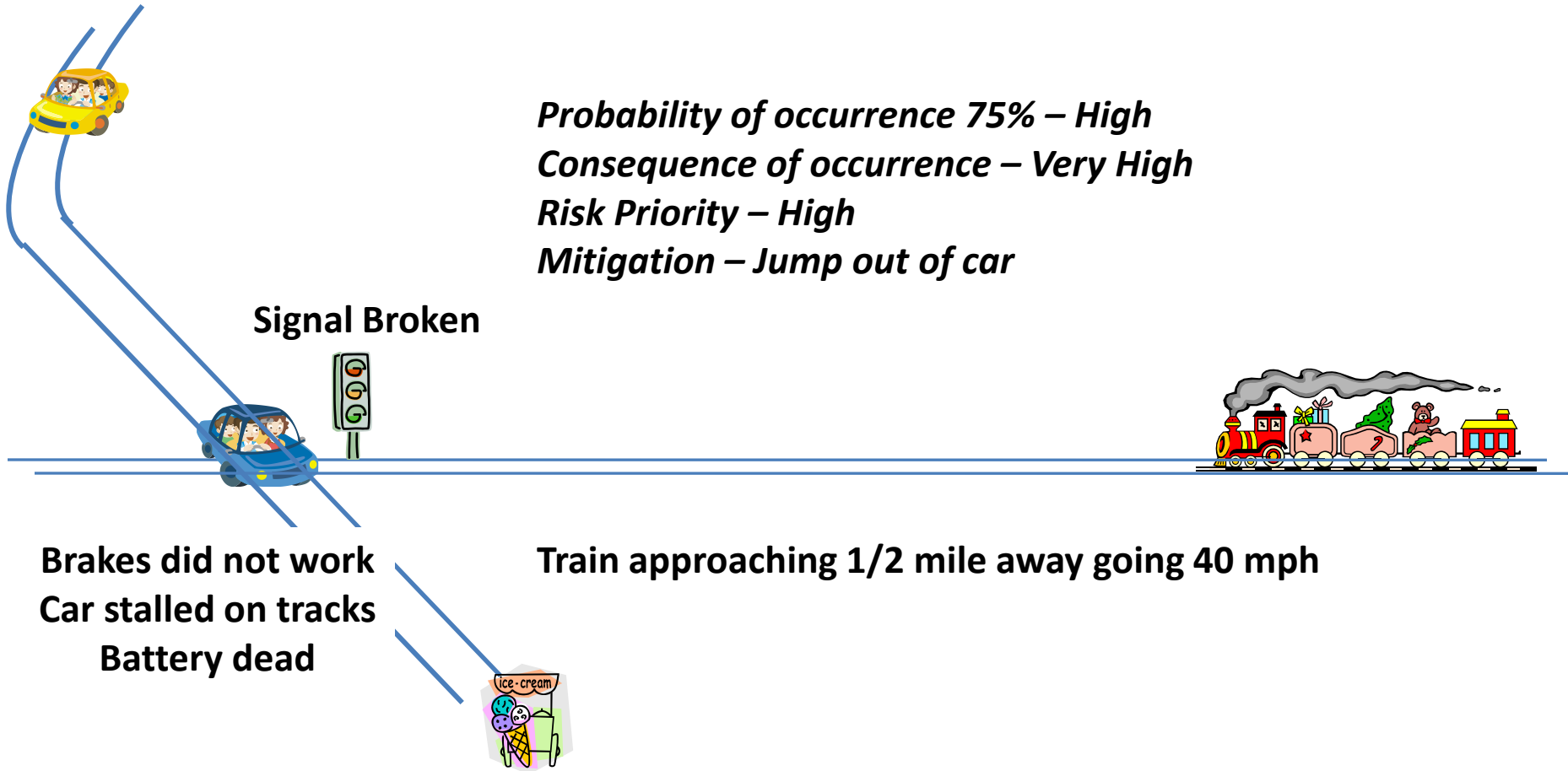
Risk Status

- Risk monitoring includes constant monitoring and providing status of the risks including
  - Analysis the current status of the risks
  - Updates the
    - Probability of occurrence
    - Impact of occurrence
    - Other risk parameters
    - Mitigation strategies
    - Contingency strategies

Risk Closure

- Risks are closed when:
  - They are no longer a threat (the risk lessened or vanished)
  - They have been mitigated
  - They have been transferred or escalated
    - The new owners now manage and monitor the risk
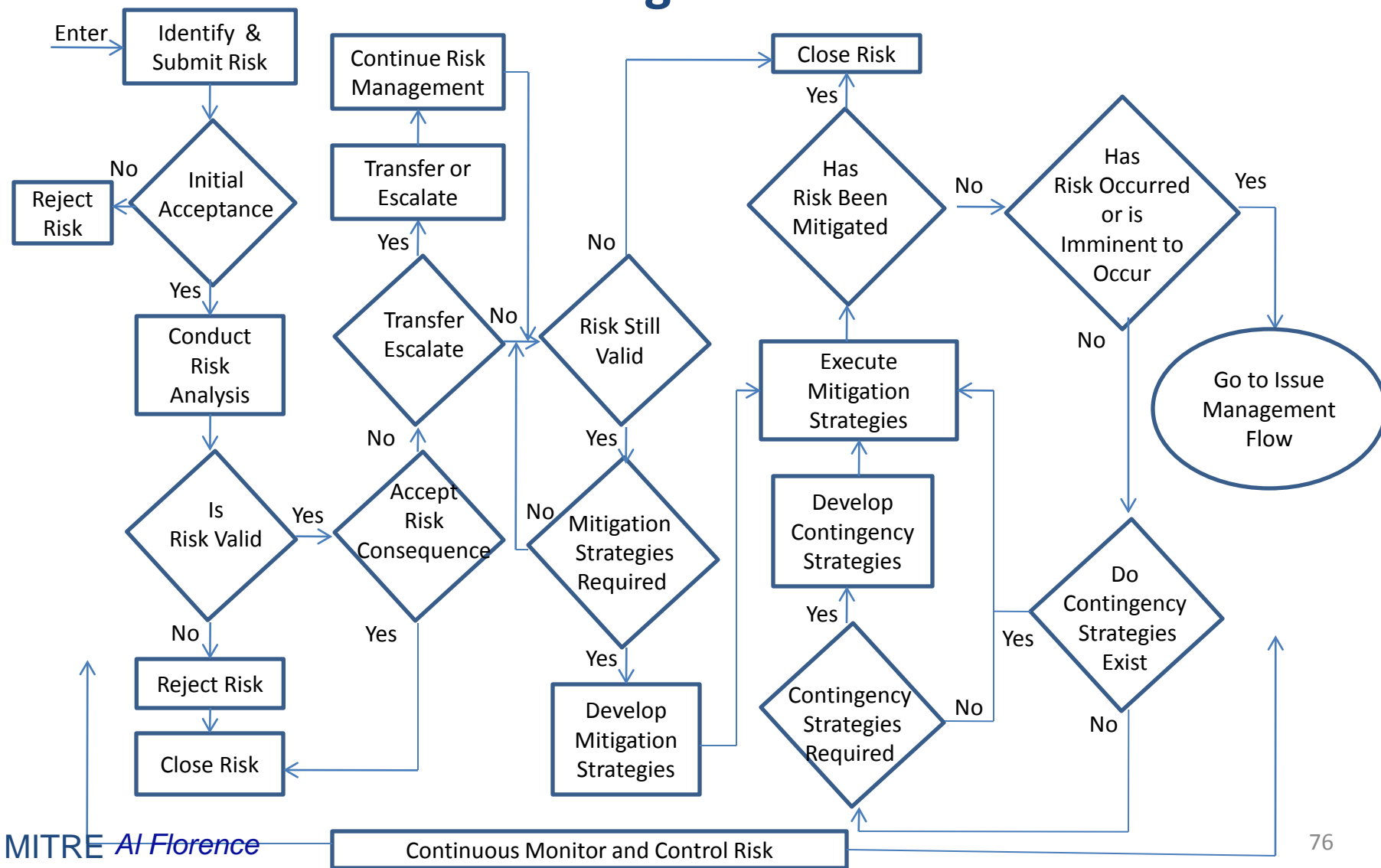- When risks occur they now become Issues and may be closed as risks or left open in the repository as Issues

Risk

Probability of occurrence 75% – High
Consequence of occurrence – Very High
Risk Priority – High
Mitigation – Jump out of car

Signal Broken

Brakes did not work
Car stalled on tracks
Battery dead

Train approaching 1/2 mile away going 40 mph

In Review
Risk Management Flow

Enter → Identify & Submit Risk

Identify & Submit Risk → Initial Acceptance
- No → Reject Risk
- Yes → Conduct Risk Analysis

Conduct Risk Analysis → Is Risk Valid
- No → Reject Risk → Close Risk
- Yes → Accept Risk Consequence

Accept Risk Consequence
- No → Transfer Escalate
- Yes → Close Risk

Transfer Escalate
- No → Risk Still Valid
- Yes → Transfer or Escalate → Continue Risk Management

Risk Still Valid
- No → Transfer Escalate
- Yes → Mitigation Strategies Required

Mitigation Strategies Required
- No → Execute Mitigation Strategies
- Yes → Develop Mitigation Strategies

Develop Mitigation Strategies → Execute Mitigation Strategies

Execute Mitigation Strategies → Has Risk Been Mitigated
- Yes → Close Risk
- No → Has Risk Occurred or is Imminent to Occur

Has Risk Occurred or is Imminent to Occur
- Yes → Go to Issue Management Flow
- No → Do Contingency Strategies Exist

Do Contingency Strategies Exist
- Yes → Develop Contingency Strategies
- No → (Continuous Monitor and Control Risk)

Contingency Strategies Required
- Yes → Develop Contingency Strategies → Execute Mitigation Strategies
- No → (Continuous Monitor and Control Risk)

Continuous Monitor and Control Risk

Where Are We

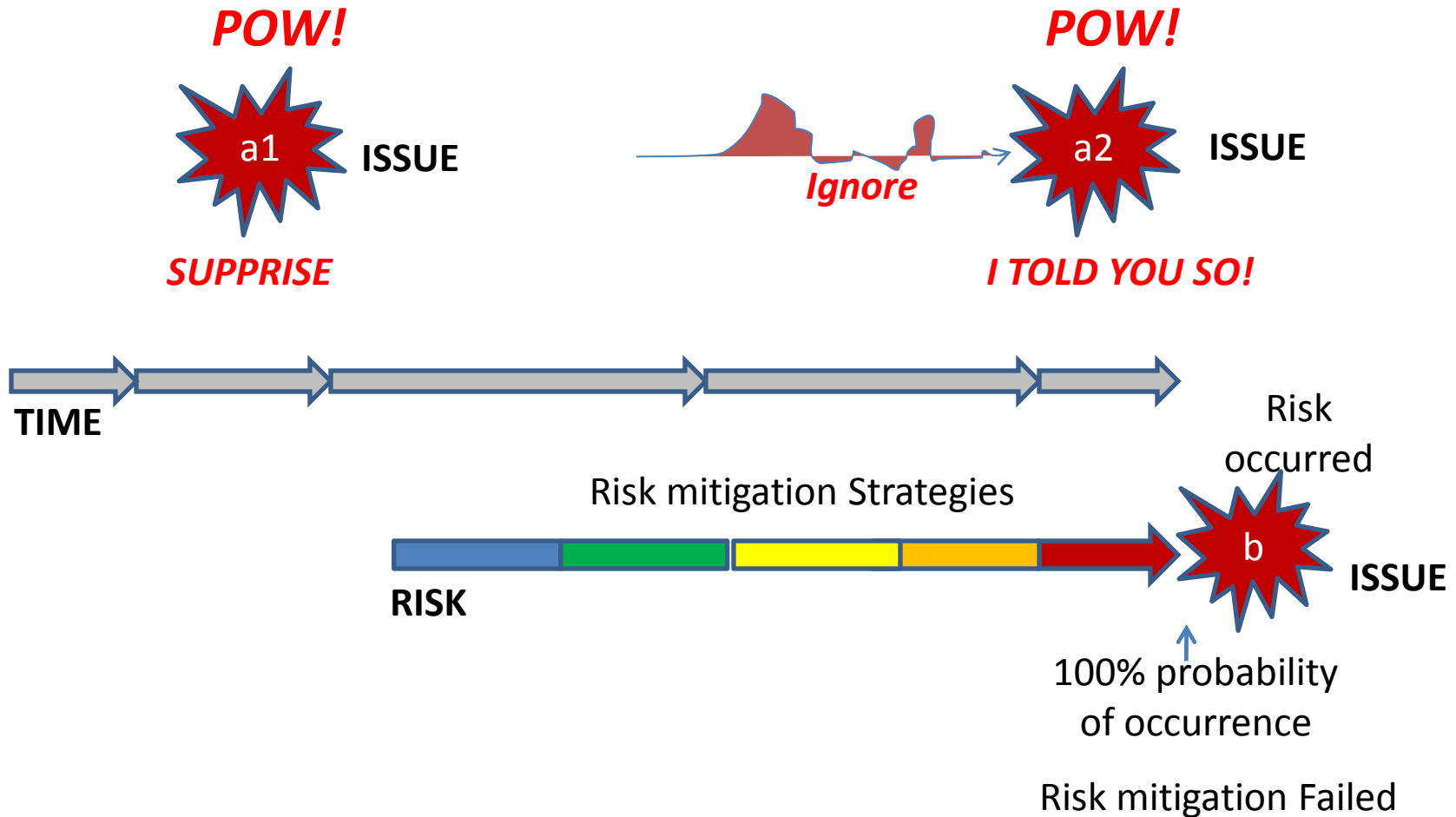- Tutorial Objectives
- Introduction
- Reasons for Risk/Issue Management
- Opportunities
- Risk Management
➡ - *Issue Management*
- Risk/Issue Avoidance
- Risk/Issue Opportunities
- Questions/ Discussion
- References
- Contact Information

MITRE *AI Florence*

Issue Management

- An issue is an event that has occurred or will *occur with certainty* and *adversely affects* the ability of the project or program to meet its objectives

  a) A formally identified adverse condition related to a program

  a1) Had not been identified as a risk prior to its occurrence

  a2) Had been identified as a risk prior to its occurrence but had not been managed as a risk

  b) A program risk that has occurred or is imminent to occur

  - Reached its probability of occurrence of 1 (one) or 100%
  - Not yet occurred but the probability of occurrence is approaching 100%
    – At this time should be managed as an issue

Used in Next slide

Some concepts from: PM@UTS Learning Program Step by step guide to project management

Issue Management

POW!

a1 **ISSUE**

SUPPRISE

POW!

Ignore

a2 **ISSUE**

I TOLD YOU SO!

TIME

Risk occurred

Risk mitigation Strategies

b **ISSUE**

RISK

100% probability of occurrence

Risk mitigation Failed

Issue Management

- If program/project issues are not addressed they may:
  - Affect program/project schedule
  - Increase program/project cost
  - Change program/project scope
  - Diminish program/project performance

- Issues can be associated with all aspects of a program (e.g., threat, technology maturity, supplier capability, design, performance against plans) as these aspects relate across the Work Breakdown Structure and Integrated Master Schedule

Issue Management Flow
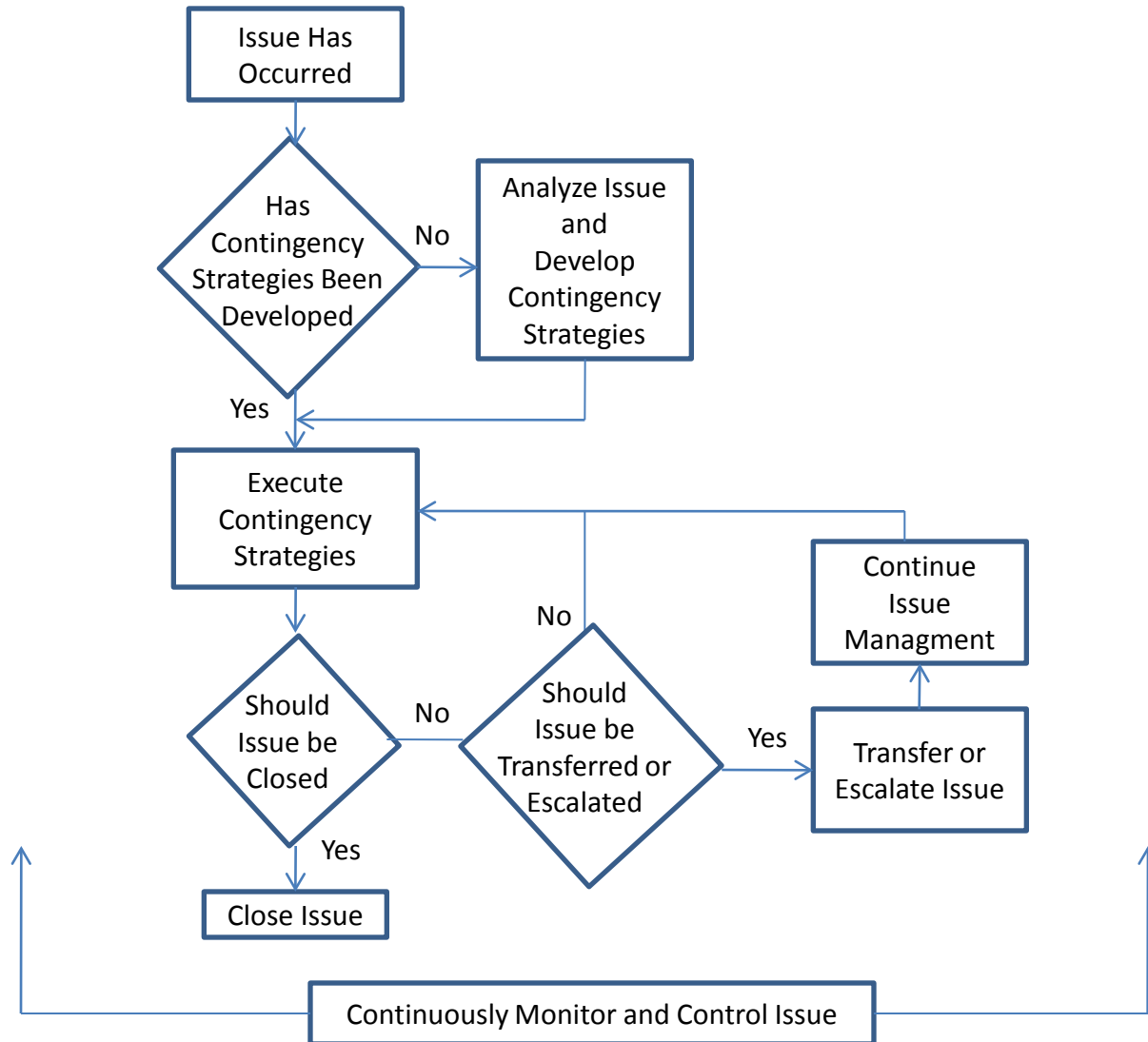
Issue Management

- Issue Management quickly identifies and effectively resolves problems as they occur and involves:
    - Issue Identification
    - Issue Analysis
    - Issue Response
    - Issue Monitoring and Control

Issue Identification

- Issue identification activities are similar to those for risk identification
- If the issue is one that occurred, without being associated with a risk, then it needs to be identification
- Issue identification would have been done if the issue resulted from a risk occurring
  - Regardless issues may need additional identification
    - Especially in identifying root causes

Issue Description

- If the issue was a risk that occurred it should have been described with the risk description

- If the issue was not related to a risk the issue needs to be described
  - The conditions that caused an issue to occur along with root cause(s) need to be identified and described
    - This includes the consequences of the issue occurrence
  - The risk writing guidelines presented earlier can be used as appropriate to issues

Issue Analysis

- Issue analysis activities are similar to those for risk analysis
  - If an issue is a risk that has occurred, some, if not all, risk analysis may be sufficient for the issue
    - The issue may need additional analysis due to its impact on program/project activities and products
  - If the issue is one that occurred without it being associated with a risk then issue analysis needs to be conducted
    - The root cause needs to be identified
    - Impact level, rated from very low (1) to very high (5), is assessed in at least four categories:
      - Cost
      - Schedule
      - Scope
      - Performance

Issue Response

- Issue response could include
  - Acceptance
    - Accept the consequence of the issue
    - Same reasons as acceptance of risks
  - Transfer
    - If the occurred risk had not been transferred the issue responsibility may now be shifted to another party who is better equipped to deal with the issue
  - Escalate
    - If the occurred risk had not been escalated the issue responsibility may now be escalated to higher authority based on threshold described earlier
  - Contingencies
    - Can be developed using the similar methods described for risk mitigations

Issue Response

- Issue contingencies are strategies to eliminate or reduce the negative effect of the issue

- Issue contingencies should have been developed for issues that were the result of a risk occurring
  - If not they need to be developed
  - They may need to be enhanced
    - If they were associated with risks earlier

- For issues that were not the result of a risk occurring contingencies need to be developed

Issue Monitoring and Control

- Issues are monitored and controlled until they are closed
- Issues are monitored and controlled using similar methods described for risk monitoring and control

Risk/Issue

Probability of occurrence 97% – Very High
Consequence of occurrence – Very High
Risk Priority – Very High
Contingency – Pray

Signal Broken
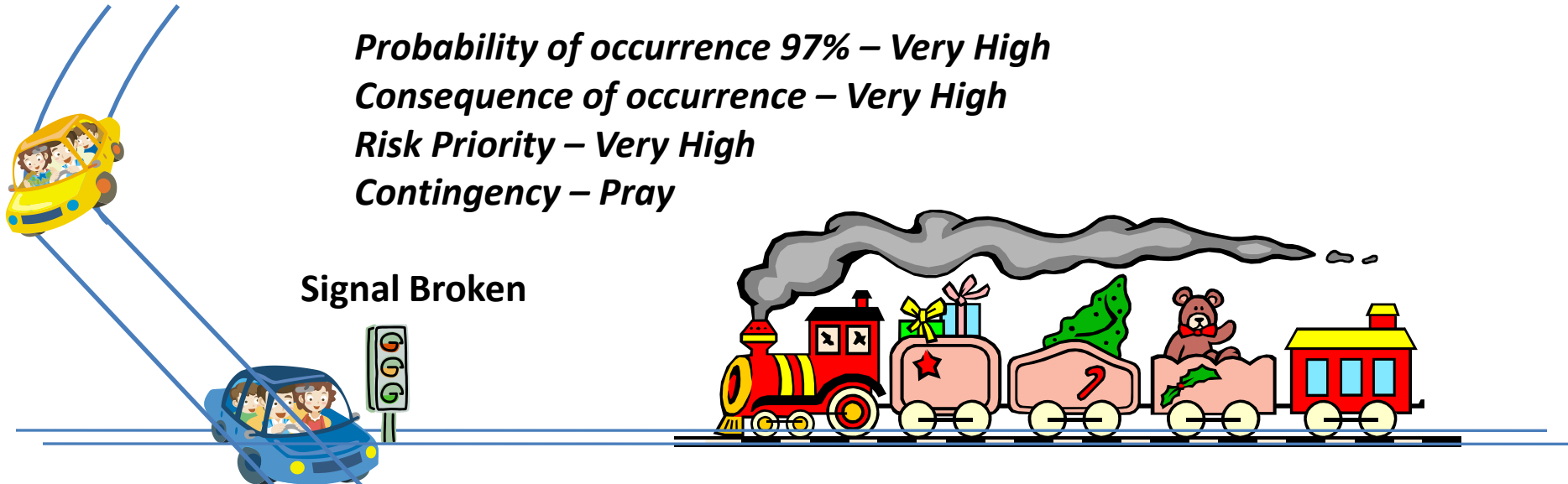
Car stalled on tracks
Battery still dead
Doors jammed

Train approaching 200 yards away going 30 mph

Murphy is for real!

Black Swan Events

The Black Swan: The Impact of the Highly Improbable;

Nassim Nicholas Taleb

WIKIPEDIA

Black Swan Events

- Black Swan Events were described by Nassim Nicholas Taleb in his 2007 book, *The Black Swan*

- Taleb regards almost all major scientific discoveries, historical events, and artistic accomplishments as "black swans"—undirected and unpredicted

- He gives the rise of the Internet, the personal computer, World War I, and the September 11, 2001 attacks as examples of Black Swan Events

We can add the 2004 Indonesian Tsunami, The Haiti Earthquake, Columbia, Challenger, Killer Whale Tilikum, Toyota Recalls-to Stock Holders and Owners, not sure about Toyota Executives - Al Florence

Black Swan Theory

- The Black Swan Theory is used by Nassim Nicholas Taleb to explain the existence and occurrence of high-impact, hard-to-predict, and rare events that are beyond the realm of normal expectations

- Such events are considered extreme outliers

Black Swan Events

- The main idea in Taleb's book is not to attempt to predict Black Swan Events
  - but to build robustness into negative ones that occur and being able to exploit positive ones
- Taleb contends that banks and trading firms are very vulnerable to hazardous Black Swan Events and are exposed to losses beyond that predicted by their defective models
  - *Sounds familiar? Al Florence*
- Taleb states that a Black Swan Event depends on the observer
  - using a simple example, what may be a Black Swan surprise for a turkey is not a Black Swan surprise for its butcher
  - hence the objective should be to "avoid being the turkey" by identifying areas of vulnerability in order to "turn the Black Swans white"

> *The same can be said about 9/11; Black Swan for Americans, White Swan for terrorists! - Al Florence*

Black Swan Bottom Line

- Black Swan Events are events that have an extremely low probability of occurrence
  - cannot be predicted
- But have a very high consequence if occur
  - positive or negative
- Mitigation is near impossible for negative ones since it is not known when, where and how or if they will occur

Al Florence

> How about an All Black Penguin?
> Discovered March 11, 2010 near Antarctica
> One in a zillion occurrence
> So, what would a All Black Penguin event be?

Where Are We

- Tutorial Objectives
- Introduction
- Reasons for Risk/Issue Management
- Opportunities
- Risk Management
- Issue Management
- ➡ ***Risk/Issue Avoidance***
- Risk/Issue Opportunities
- Questions/ Discussion
- References
- Contact Information

MITRE *AI Florence*

Risk/Issue Avoidance

- Risk/Issue Avoidance has at least two components:
  - Eliminate the sources of high risks and issues and replace them with a lower-risk alternatives
  - The establishment of sound technical, programmatic and management processes, and activities early and their continued execution throughout the entire lifecycle
    - This helps remove common risks/issues root causes

Low-Risk Alternatives

- Eliminate the sources of high risk and replace them with a lower-risk alternatives

  - The selection and implementation of alternative activities or products without, or with lower, risk to replace the riskier activities or products

  - These alternatives may eliminate or reduce the impact if the risk occurs

Alternative Approaches

- Risk analysis and mitigation involves the investigation and implementation of alternative approaches which may include:
  - Technical
    - Example: substitute COTS products, relax requirements
  - Management
    - Example: reassign tasks, augment teams
  - Programmatic
    - Example: manipulate schedules, reduce documentation, increase budgets

Industry Best Practices

- Implementing industry best practices within organizations and executing them on projects can drastically reduce risks and issues

- Best practices include technical and programmatic processes and procedures

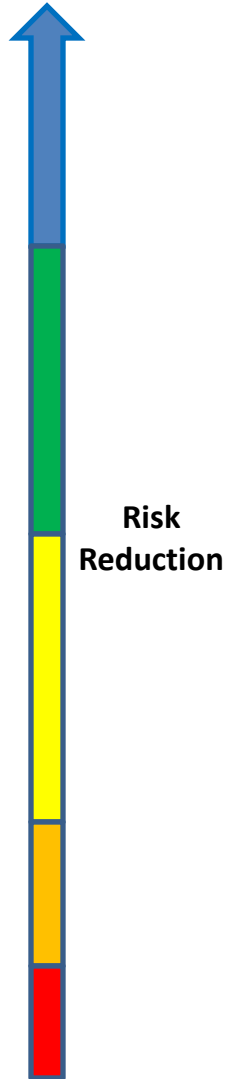By doing this organizations will go a long way in reducing risk and issues

SEI CMMI

- Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI)
  - CMMI for Development v1.2– For suppliers developing/supplying
    - Software
    - Hardware
    - Systems
    - Commercial of the Shelf (COTS)
  - CMMI for Acquisition v1.2
    - For customers acquiring systems, products and services
  - CMMI for Service v1.2
    - For organizations providing services

All these CMMIs have process areas for most activities associated with program/project development and acquisition
Their proper implementation would result in best practices

SEI CMMI

CMMI Process Areas for CMMI for Development v1.2

Level	Process Areas
5 - Optimizing	Organizational Innovation and Deployment Causal Analysis and Resolution
4 - Quantitative Managed	Organizational Process Performance Quantitative Project Management
3 - Defined	Requirements Development Technical Solution Product Integration Verification Validation Organizational Process Focus Organizational Process Definition Organizational Training Integrated Project Management Risk Management Decision Analysis and Resolution
2 - Managed	Requirements Management Project Planning Project Monitoring and Control Supplier Agreement Management Measurement and Analysis Process and Product Quality Assurance Configuration Management

1 - Initial Competent people and heroics, sometimes ad hoc *(Subject to high incidence of RISKS)*

Risk Reduction

MITRE *AI Florence*

SEI CMMI

The CMMI is itself a Risk Management Plan

Managing Risks, Methods for Software Systems Development; Dr. Elaine M. Hall, SEI Series in Software Engineering

Other Frameworks

- Other Methodologies/Frameworks
  - 6 Sigma
    - Process Improvement
    - Reduce variation
    - Statistical/quantitative
  - Lean 6 Sigma
    - Process Improvement
    - Reduce Waste
    - Less statistically rigorous then 6 sigma
  - ITIL – Information Technology Infrastructure Library
    - For Information Technology
    - Services Focused

Other Frameworks

– ISO 9000 standards

- ISO 9001 - applies to companies required to design, develop, produce, install, service and supply a product or service

- ISO 9002 - applies to companies required to produce, install, service and supply a product or service according to an existing design

- ISO 9003 - addresses only the requirements for detection and control of problems during final inspection and testing

– Others

Reducing Risks with the Proper Specification of Requirements

The next presentation was published as a paper in Crosstalk, The Journal of Defense Software Engineering, April 2002 by Al Florence
Title of the publication:

RISKY Requirements

It also received an award in the best paper competition at MITRE

December 17, 2008 — **Computerworld** —
Melinda-Carol Ballou, an analyst with IDC in Framingham, Mass., said that 70% to 80% of IT project failures relate directly to poor requirements gathering, management and analysis.

And specification – Al Florence

MITRE *Al Florence*

Proper Specification of Requirements

- A government agency, while modernizing their information systems, reverse-engineered requirements
- With domain knowledge of the application, several teams were involved
  - They represented
    - Users
    - Contractors
    - Acquisition organization
- This author was assigned as a consultant to guide the teams in the proper specification of requirements
- The examples presented show some of the requirements:
  - As initially specified by the teams
  - Next a critique of the requirements by this author
  - Finally the re-specified requirements based on the critique

MITRE *AI Florence*

Criteria for Specifying a Good Requirement

The following are some critical attributes that requirements must adhere to: *(Used to critique requirements)*

- Completeness: Requirements should be complete

  They should reflect system objectives and specify the relationship between the software and the rest of the subsystems

- Consistency: Requirements must be consistent with each other; no requirement should conflict with any other requirement

  Requirements should be checked by examining all requirements in relation to each other for consistency and compatibility

Criteria for Specifying a Good Requirement

- Traceability: Each requirement must be traceable to some higher-level source, such as a system level requirement

  Each requirement should also be traced to lower level design and test abstractions such as high-level and detailed-level design and test cases

- Testability: All requirements must be testable in order to demonstrate that the software end product satisfies its requirements

  In order for requirements to be testable they must be specific, unambiguous, and quantitative whenever possible. Avoid negative, vague and general statements

Criteria for Specifying a Good Requirement

- Feasibility: Each requirement must be feasible to implement

    Requirements that have questionable feasibility should be analyzed during requirements analysis to prove their feasibility

- Unique identification: Uniquely identifying each requirement is essential if requirements are to be traceable and testable

    Uniqueness also helps in stating requirements in a clear and consistent fashion

Criteria for Specifying a Good Requirement

- Design Free: Software requirements should be specified at a requirements level not at a design level

    The approach should be to describe the software requirement functionally from a system (external) point of view, not from a software design point-of-view, i.e. describe the system functions that the software must satisfy. Some requirements may have design embedded due to constraints placed on them by the system, interfaces or legacy

- Use of "shall" and related words: In specifications, the use of the word "shall" indicates a binding provision

    Binding provisions must be implemented by users of specifications. To state non-binding provisions, use "should" or "may". Use "will" to express a declaration of purpose (e.g., "The Government will furnish..."), or to express future tense.   MIL-STDs

> *Note: Methods other that the use of "shall" can be used to specify requirements such as using a matrix with a column for requirements and another column for comments or italics or underlines for comments.*

Example 1

- Initial specification

    The Financial Agent sends to the government by 6:00 PM ET on the same day after receipt of the file CRDF that includes only critical data collected from the enrolled individual.

- Critique

    - No unique identifier provided

    - The word "shall" is missing

    - How is the file sent?

    - Has design implications: "CRDF"

        - Should define data, not name of data file - this should be done in the design

    - The critical data has to be identified

Example 1

- Re-specification

  3.3.1.3   The Financial Agent shall send the government, via electronic transmission, the following critical data collected from each enrolled individuals by 6:00 PM ET on the day of receipt:

  a. Name

  b. Address

  c. Zip Code

  d. Social Security Number

Example 2

- Initial specification:

  3.2.5.7 The system shall process two new fields (provides production count balancing info to states) at the end-of-state record

- Critique:
  - This requirement cannot be implemented or tested.
  - It is incomplete. What are the two new fields?
  - "Info" should be spelled out

- Re-specification:

  3.2.5.7 The system shall provide the following data items (provides production count balancing information to states) at the end-of-state record:

    a. SDATE, and
    b. YR-TO-DATE-COUNT

Example 2

- Re-Critique:
  - This rewrite has design implications SDATE record and YR-TO-DATE-COUNT
    - From a requirements viewpoint it should specify what the data in the records are, not the name of the record as it exists in the design and implementation

- Re-Re-Specification:

3.2.5.7 The system shall provide the following data items (provides production count balancing information to states) at the end-of-state record:

a. Submission date and time

b. Year-to-date totals

Example 3

- Initial specification:

  3.2.5.9 All computer-resident information that is sensitive shall have system access controls. Access controls shall be consistent with the information being protected and the computer system hosting the data.

- Critique:
  - Two "shalls" under one identifier
  - The requirement is vague and incomplete. Need to identify the sensitive information.
  - What does "consistent" mean?
  - As specified it cannot be implemented or tested

- Re-specification:

  3.2.5.9 All sensitive computer-resident information shall have system access controls, consistent with the level of protection. (Reference Sensitive Information, Table 5.4.1 and Level of Protection for Sensitive Information, Table 5.4.2)

Example 4

- Initial specification:

Software will not be loaded from unknown sources onto the system without first having the software tested and approved

- Critique:
  - If it is tested and approved, can it be loaded from unknown sources?
  - If the source is known, can it be loaded without being tested and approved?
  - Requirement is ambiguous and stated as a negative requirement, which makes it difficult to implement and test
  - A unique identifier is not provided, which makes it difficult to trace
  - The word "shall" is missing

MITRE *AI Florence*

Example 4

- Re-specification:

3.2.5.2 Software shall be loaded onto the operational system only after it has been tested and approved

Example 5

- Initial specification:

  3.2.7.1 The system shall purge state control records and files that are older than the operator or technical user-specified retention period

- Critique:
  - Requirement is incomplete and vague without specifying the retention period or providing a reference as to where the information can be obtained
  - Requirement cannot be implemented or tested as stated

- Re-specification:

  3.2.7.1 The system shall purge state control records and files that are older than the retention period input into the system by either the
  - a. operator, or
  - b. technical user

Example 6

- Initial specification:

  3.3.2.1 The system shall have no single point failures

- Critique:
  - This is an ambiguous requirement. Needs identification of what components and/or functions the "no single point failures" applies to
  - As specified it cannot be implemented or tested

- Re-specification:

  3.3.2.1 The following system components shall have no single point failures:

  a. Host servers   e. Hubs
  b. Networks   f. Switches
  c. Network routers   g. Firewalls
  d. Access servers   h. Storage devices

Example 7

- Initial specification:

  3.2.6.3 The system shall receive and process state return data from the State Processing Subsystem. The system shall provide maintenance of the state data files and generate various reports.

- Critique:
  - Two "shalls" under one requirement number and multiple requirements in the specification
  - The word "process" in the first shall is vague; need to define the processing required

  - The second "shall" does not provide for valid requirements; they cannot be implemented or tested as stated
    - Needs identification of type/amount of maintenance required
    - "various reports" is ambiguous

Example 7

- Re-specification:

3.2.6.3 The system shall receive:

     a. production data that contains data from multiple states, and

     b. state total amount for one or more states,

extracted by the Returns Processing Subsystem.

3.2.6.4 The system shall parse multi-state data to respective state files

3.2.6.5 The system shall display a summary screen reporting the results of processing for each state containing:

     a. state totals,

     b. state generic totals, and

     c. state unformatted totals.

Example 8

- Initial specification:

    3.2.9.1 When doing calculations the software shall produce correct results.

- Critique:
    - Really? This is not a requirement.
    - This type of non-requirements should not be specified!
    - It should be deleted.

- Re-specification:

    Requirement deleted.

Where Are We

- Tutorial Objectives
- Introduction
- Reasons for Risk/Issue Management
- Opportunities
- Risk Management
- Issue Management
- Risk/Issue Avoidance
- ***Risk/Issue Opportunities***
- Questions/ Discussion
- References
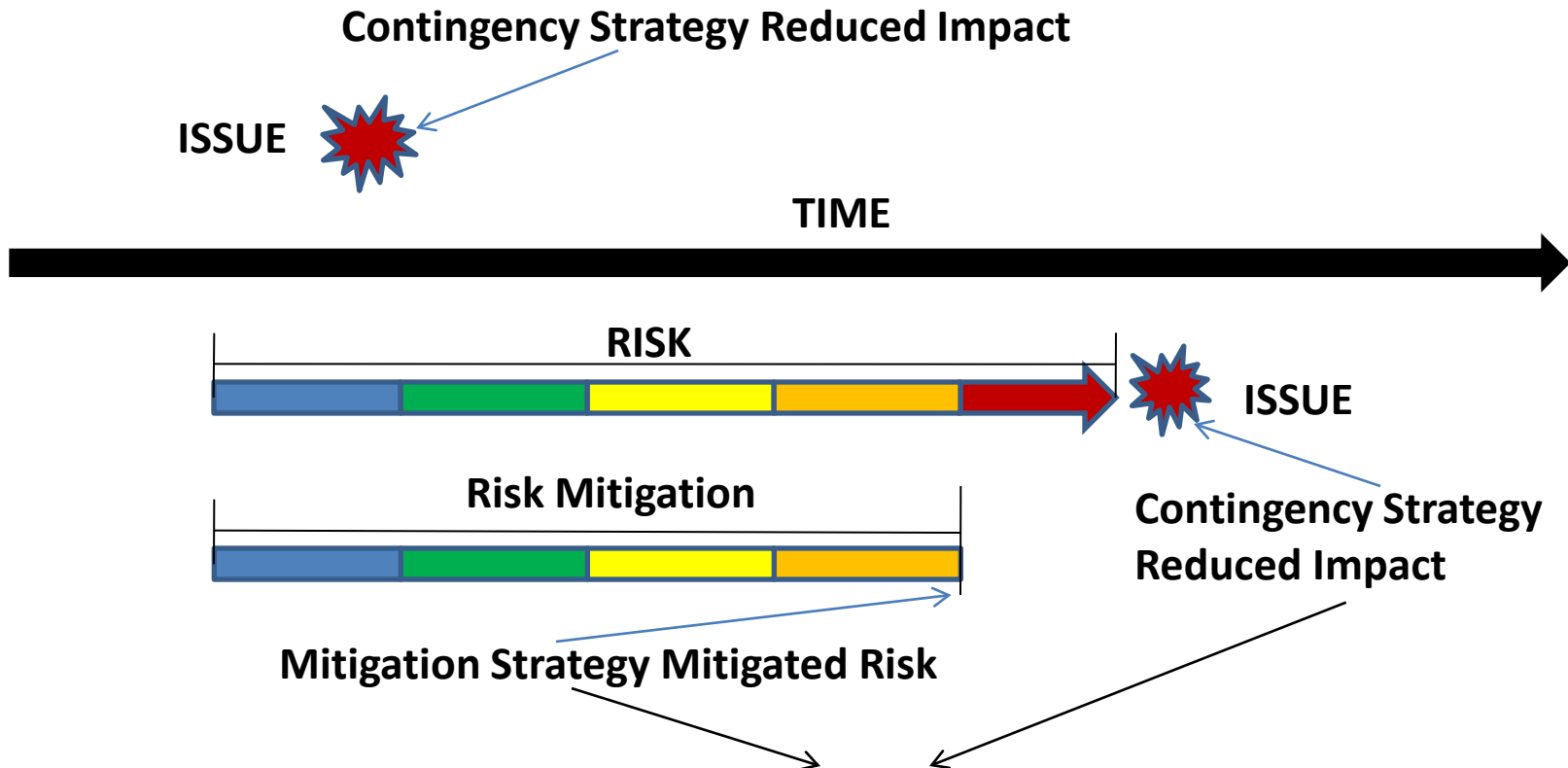- Contact Information

Risk/Issue Opportunity

- An Opportunity is a *potential* event which, if *taken advantage* of, will *positively affects* the ability of the project or program to meet its objectives
    - Opportunities to improve project performance may surface while applying mitigation or contingency strategies
    - The mitigation or contingency strategies could be used as best practices on the project or other projects to keep the risk from recurring

Risk / Opportunity

- An opportunity may be the potential of improving the value of project results; the project itself is the paramount opportunity

- A risk is the potential of not achieving the project strategic opportunity

- Taking risks can lead to opportunities but risk taking can itself be quite risky unless the risk is well thought out and well managed

Capturing Lesson Learned in Support of Opportunities

Contingency Strategy Reduced Impact

ISSUE

TIME

RISK

ISSUE

Contingency Strategy Reduced Impact

Risk Mitigation

Mitigation Strategy Mitigated Risk

Stored in lessons learned database which can be documented as a best practice opportunity to be reused on this or other projects to keep the risk or issue from recurring *(Hopefully Identified and corrected Root Cause) (Also Called Process Improvement)*

MITRE *AI Florence*

Real Project Example

- Opportunity
  - Galileo Space Probe to Jupiter to investigate the Jovian atmosphere and gather scientific information
- A Risk
  - Voyager Space Craft on flyby of Jupiter discovered high radiation, which destroys electrical components, and high incidences of cosmic ray events, which flips volatile computer bits
  - IF the Galileo Probe is not designed to protected against this phenomena prior to launch
  - THEN the microprocessor may fail before the mission is accomplished resulting in less science collected or complete mission failure
- A mitigation strategy was developed and deployed
  - Redesign the configuration of the probe to protect volatile bits and electronic components
- Issue
  - Did not materialize
- Opportunities
  - Galileo Probe was successful and accomplished its full mission
  - Lessons learned were used on other space missions
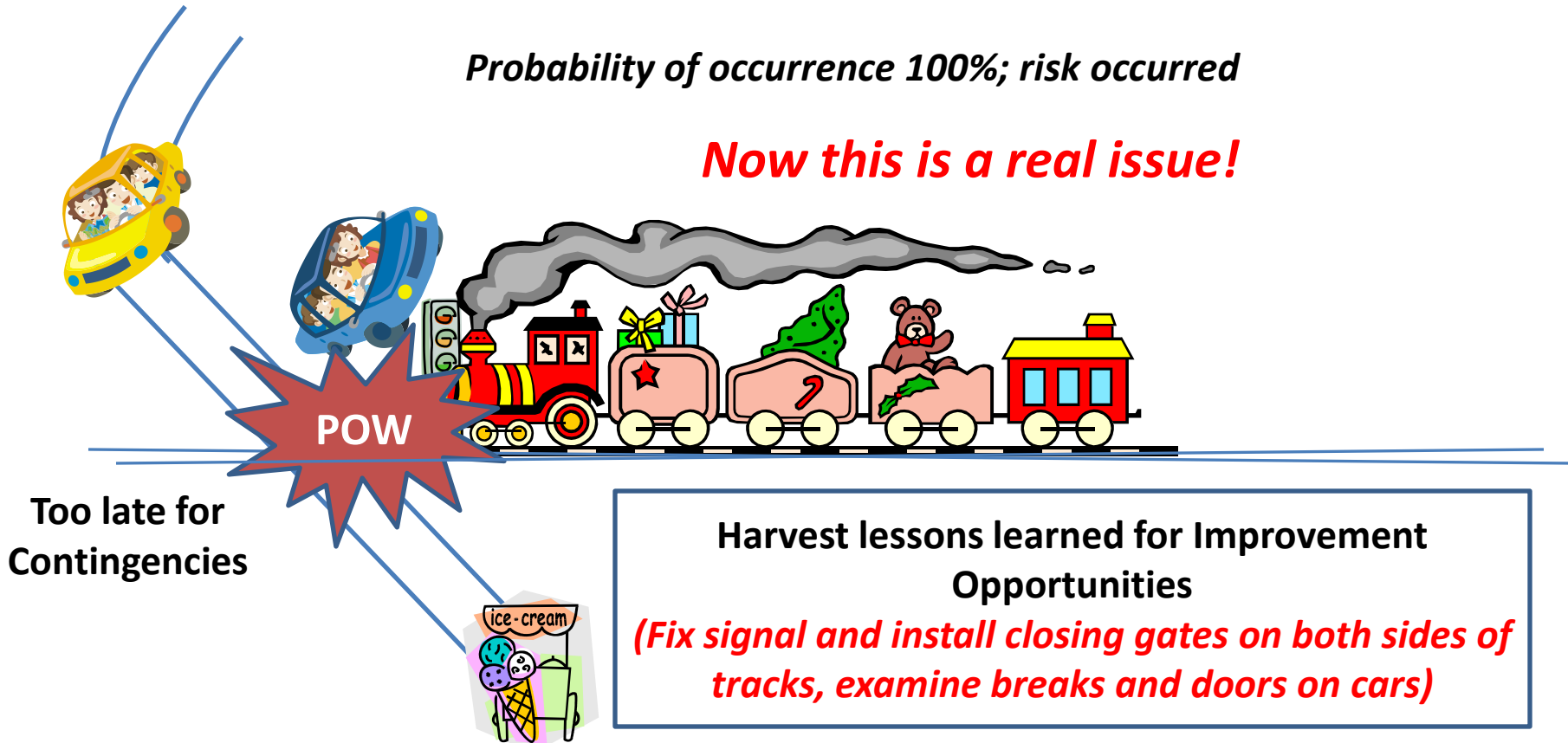
Real Project Example

- Mitigation
  - Initial design had one microprocessor to command and control the instruments, collect scientific data and telemeter to orbiter
  - Eliminate 2 experiments and install 2nd microprocessor
    - Both redundantly collecting same data and sending to orbiter
    - Place processors in the center of probe
  - Provide for redundant triple collection and triple voting on both processors on critical parameters such as timing
  - Hopefully when one processor destroyed the other may continue to operate

This mitigation (redesign) extended the life of science gathering until probe implosion

Issue/Opportunity

Probability of occurrence 100%; risk occurred

Now this is a real issue!

Too late for Contingencies

POW

Harvest lessons learned for Improvement Opportunities
(Fix signal and install closing gates on both sides of tracks, examine breaks and doors on cars)

The good news is that no one was hurt, obviously this is a toy train and toy cars

Where Are We

- Tutorial Objectives
- Introduction
- Reasons for Risk/Issue Management
- Opportunities
- Risk Management
- Issue Management
- Risk/Issue Avoidance
- Risk/Issue Opportunities
- ***Questions/Discussion***
- ***References***
- ***Contact Information***

MITRE *AI Florence*

MITRE *AI Florence*

131

References

- *IEEE/EIA 12207.2-1997 Annex L—Risk Management Implementing a Risk Management Process for a Large Scale Information System Upgrade – A Case Study;* Paul R. Garvey, The MITRE Corporation, INCOSE/PMI Risk Management Symposium 9 & 10 May 2001, INCOSE *INSIGHT*, Vo1 4. Issue 1, April 2001

- *Managing Risks, Methods for Software Systems Development,;* SEI Series in Software Engineering, Elaine M. Hall, 1998 Addison-Wesley

- *Reducing Risks with the Proper Specification of Requirements;* Al Florence; Risky Requirements, Crosstalk, The Journal of Defense software Engineering, April 2000

- *Project Management Body of Knowledge (PMBOK)*

- *Issue Management Plan Preparation Guidelines;* QATAR National Project Management

References

- *Capability Maturity Model Integration (CMMI)*
  - *CMMI for Development v1.2*
  - *CMMI for Acquisition v1.2*
  - *CMMI for Service v1.2*

  Software Engineering Institute (SEI)

- *IEEE Std 1540-2004, IEEE Standard for Software Life Cycle Processes—Risk Management;* IEEE

- *Issue Management Plan Preparation Guidelines;* QATAR National Project Management

- *The Black Swan: The Impact of the Highly Improbabl*e; Nazism Nicholas Tale ; The Random House Publishing Company

- http://pascal.computer.org/sev_display/index.action SEVOCAB: Software and Systems Engineering Vocabulary

Contact Information

Me

Al Florence

florence@mitre.org

703 983 7476