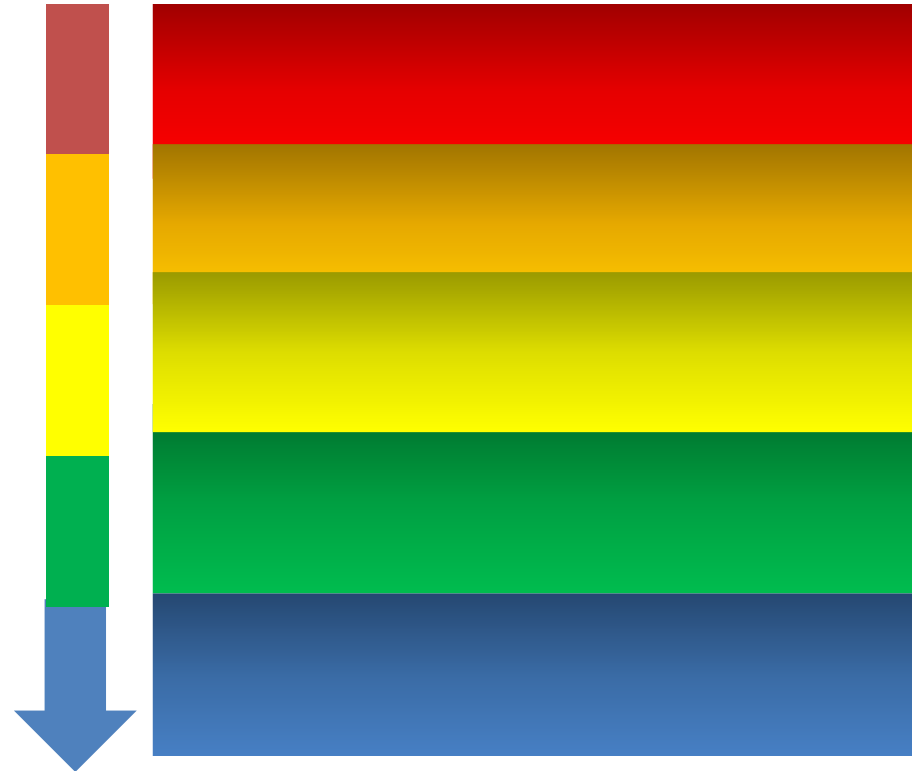


# Risk Management



Software SIG  
The MITRE Corporation  
February 26, 2013

Alfred (AI) Florence  
The MITRE Corporation

# Agenda

- • ***Introduction***
- Risk Management
- References
- Contact Information

# Introduction

## Definitions

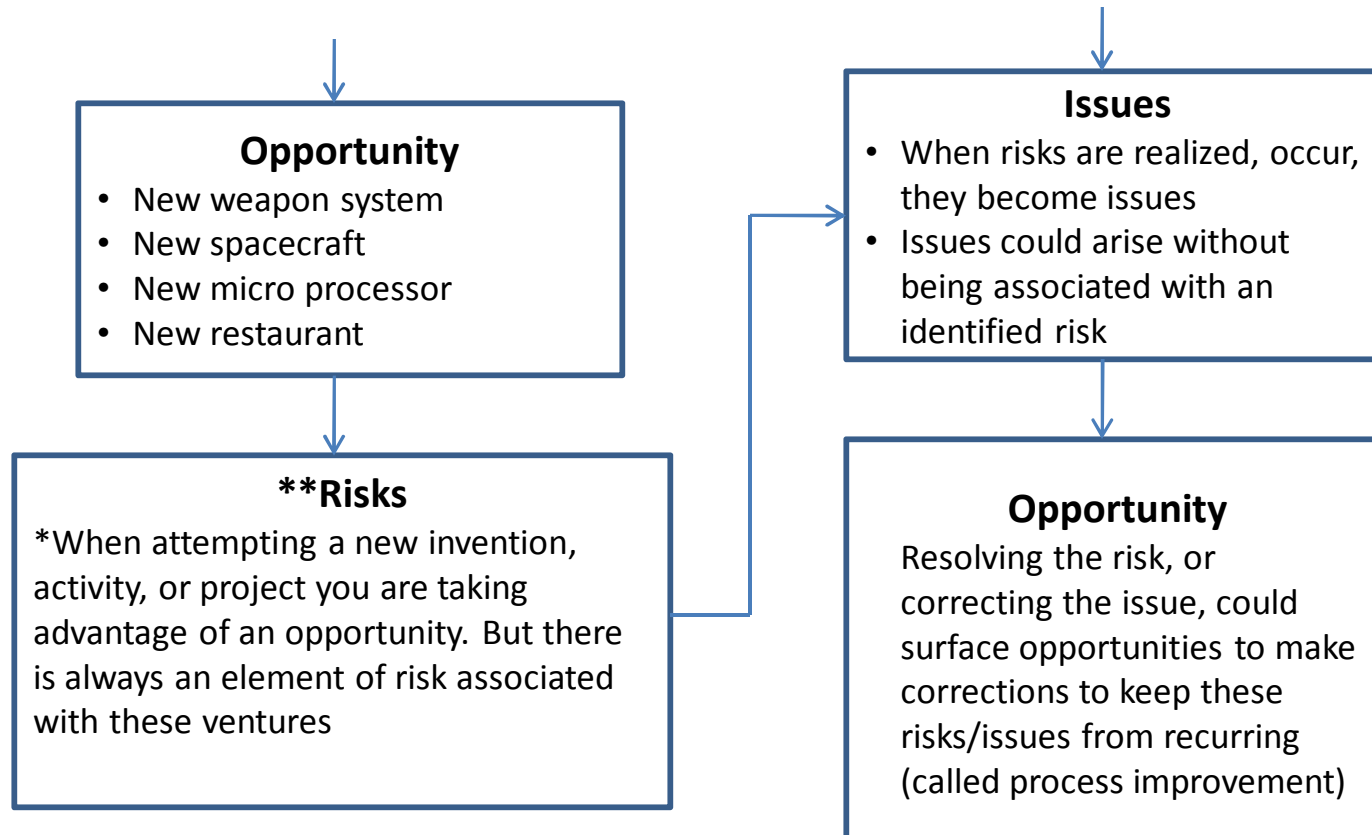
- Risks (IEEE Std 1540-2004; Standard for Software Life Cycle Processes)
  - Program and project risks are the likelihood of an event, hazard, threat, or situation occurring and its undesirable consequences
- Risk (Project Management Body of Knowledge PMBOK)
  - An uncertain even or condition that, if 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

# Introduction



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

*\*\*Focus of this presentation*

# Where Are We

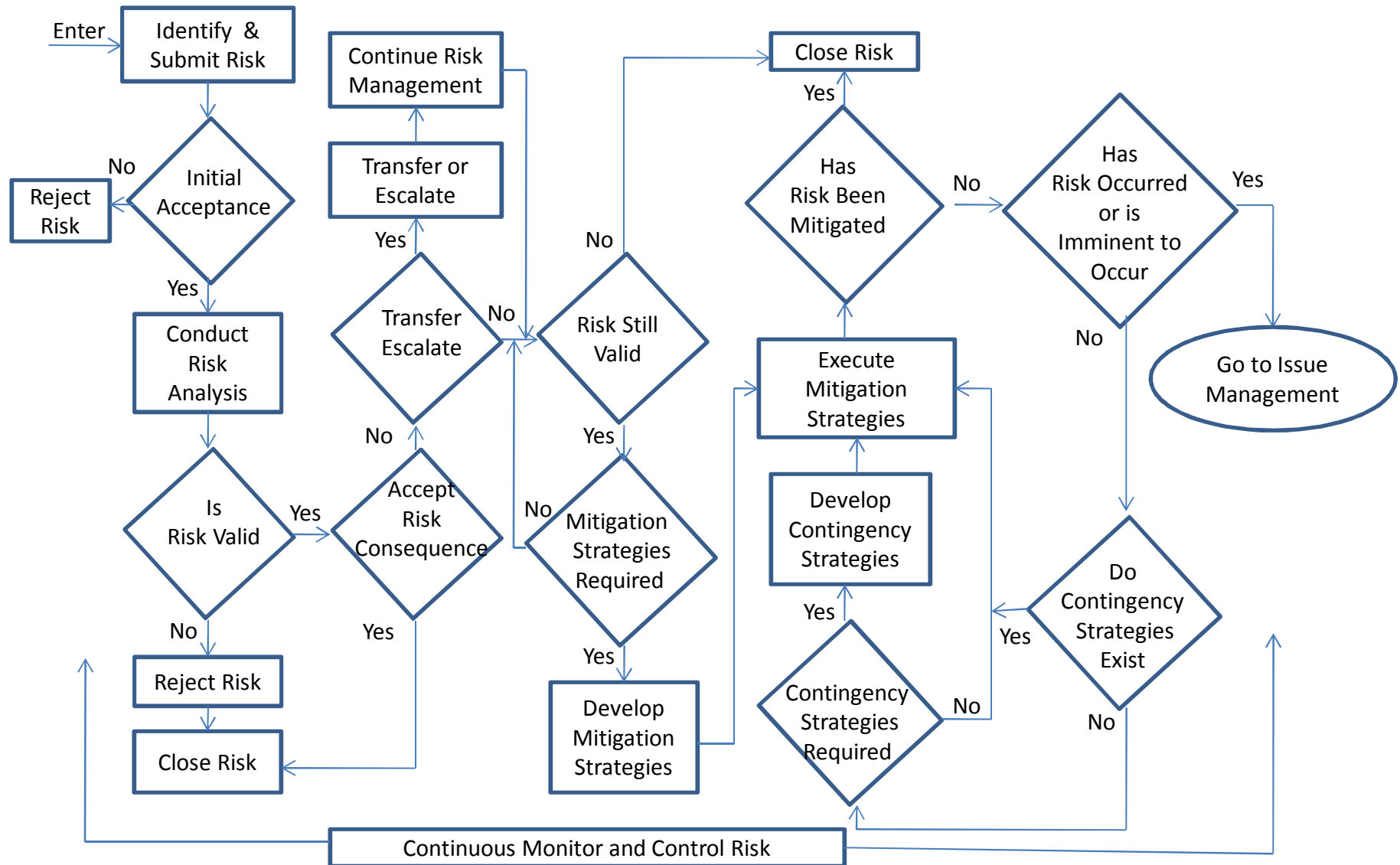
- Introduction
- • ***Risk Management***
- References
- Contact Information

# Risk Management Process

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

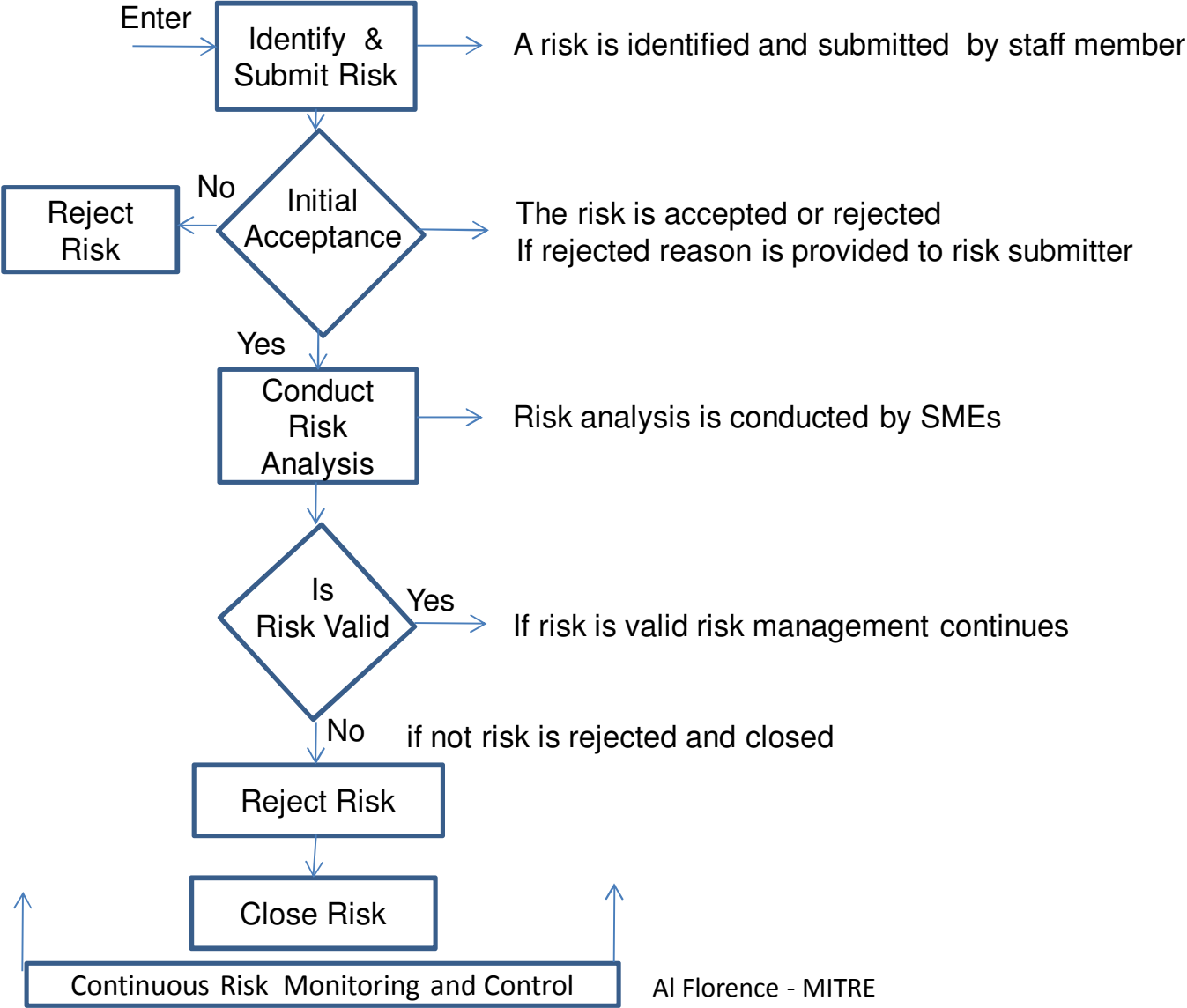
PMBOK

# Risk Management Flow

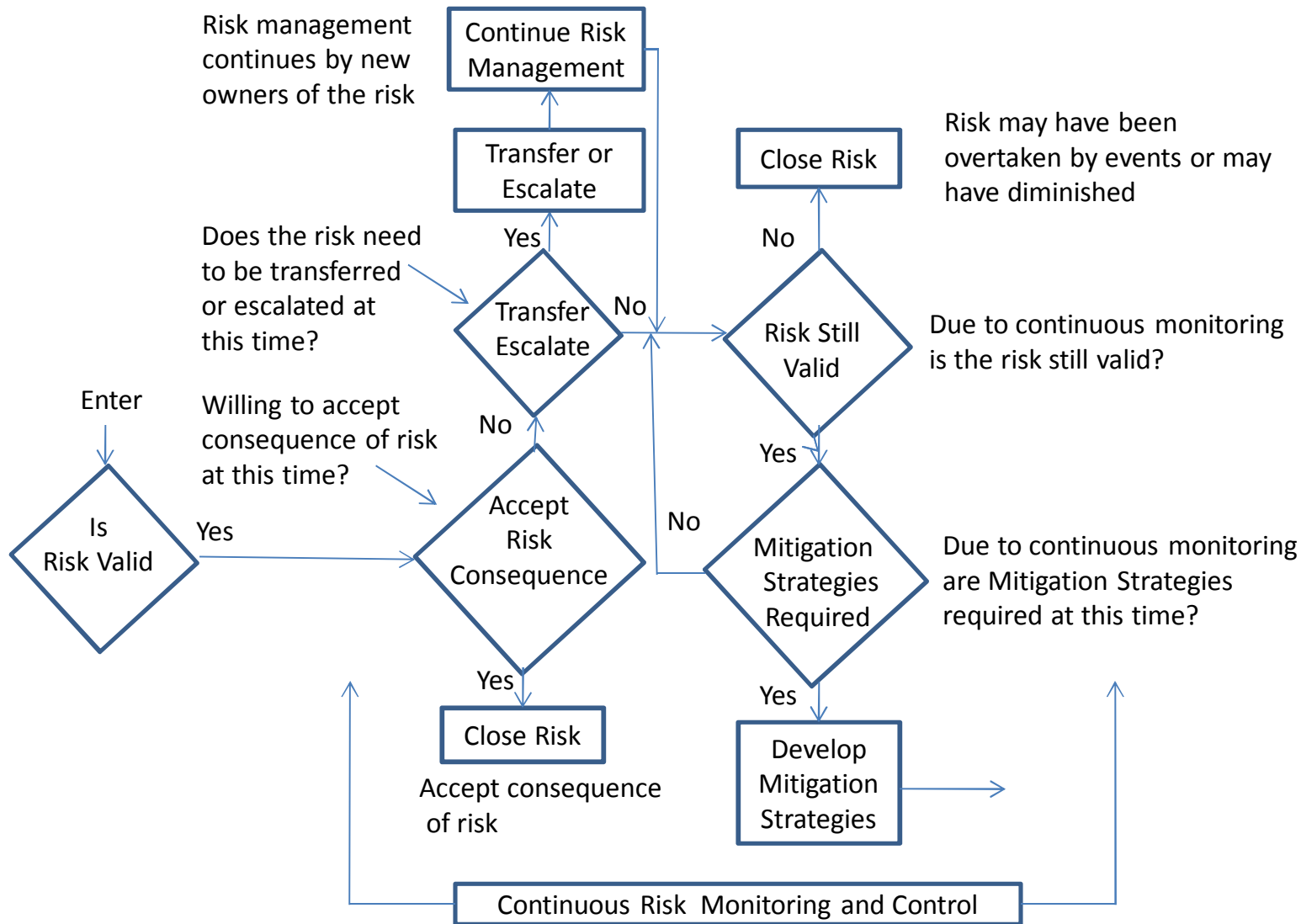




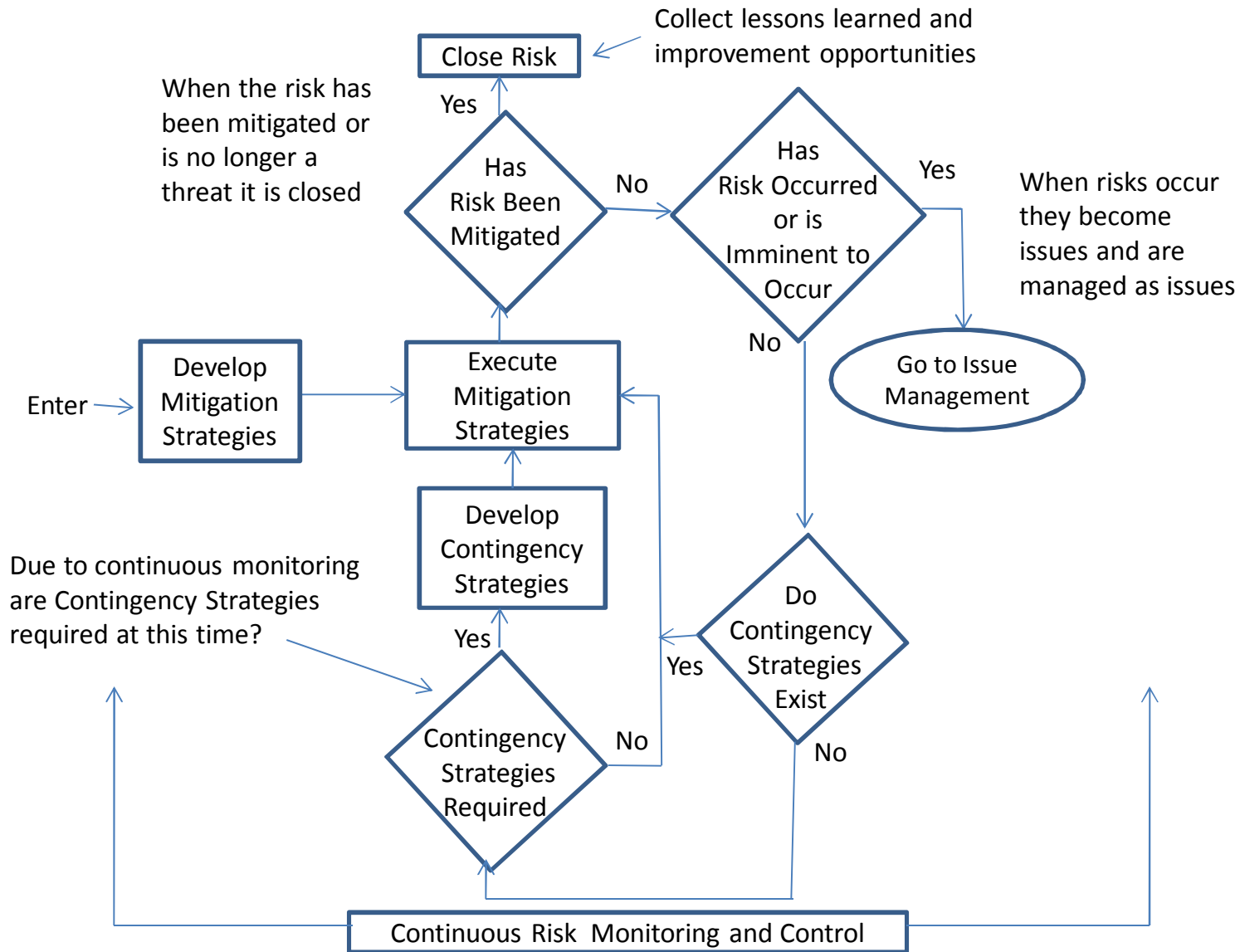
# Risk Management Flow



# Risk Management Flow



# Risk Management Flow



# 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 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 Training
- Glossary
- References

# 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
  - Risk identification begins as early as possible in successful programs and continues throughout the life of the program
- Risk can be associated with all aspects of a program; e.g.

Requirements	Design
Threat	Schedule
Security	Cost
Technology maturity	Performance
Supplier capability	Etc.

# Risk Description

- A well-written risk statement contains three main components:
  - **Cause** – The negative conditions 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 likelihood of the occurrence of the risk
    - Within a future time frame
    - Or a future event
  - **Consequence** – The effect(s), 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 2/26/2013;  
**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 2/26/2013? *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

- 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
  - 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

Also:

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

# Risk Analysis

- The risk is submitted to the Risk Management Board
- The risk is accepted or declined by the Board
  - If declined rationale 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

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

# 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)	$\geq 81\%$ and $= 100\%$
High (Probable)	61% – 80%
Medium (Possible)	41% – 60%
Low (Unlikely)	21% – 40%
Very Low (Highly improbable)	$> 1\%$ – $\leq 20\%$

# 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

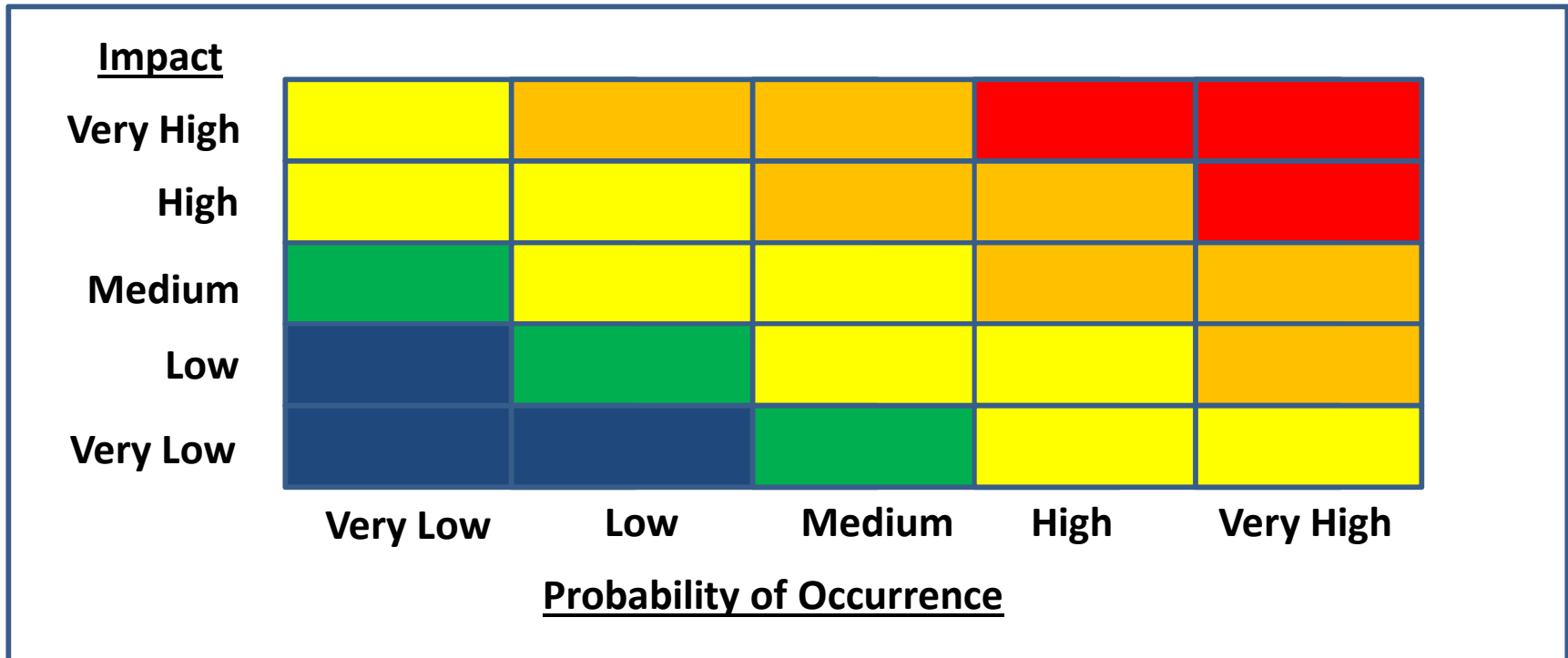
# Consequence of Risk Occurrence


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

# 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



  
Very Low  
Priority

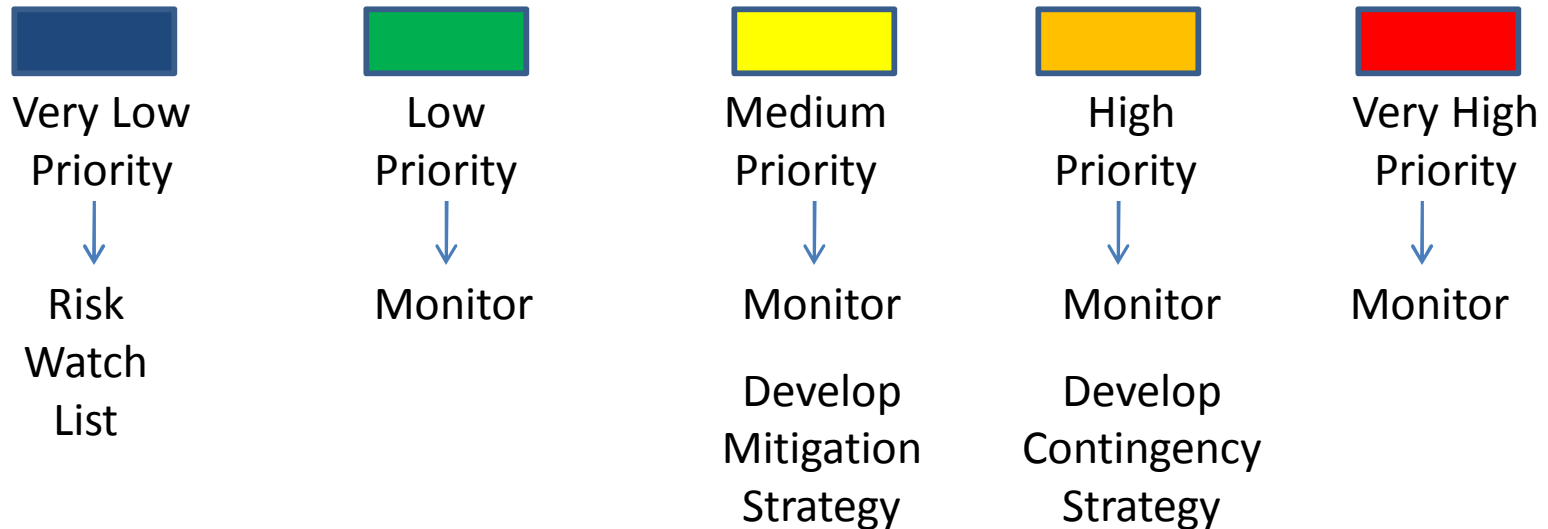
  
Low  
Priority

  
Medium  
Priority

  
High  
Priority

  
Very High  
Priority

# Risk Priority vs. Mitigation/Contingency



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

# 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

PMBOK



# 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

- Eliminate the sources of high risk and replace them with a lower-risk alternative
- Avoid risks 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 than 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

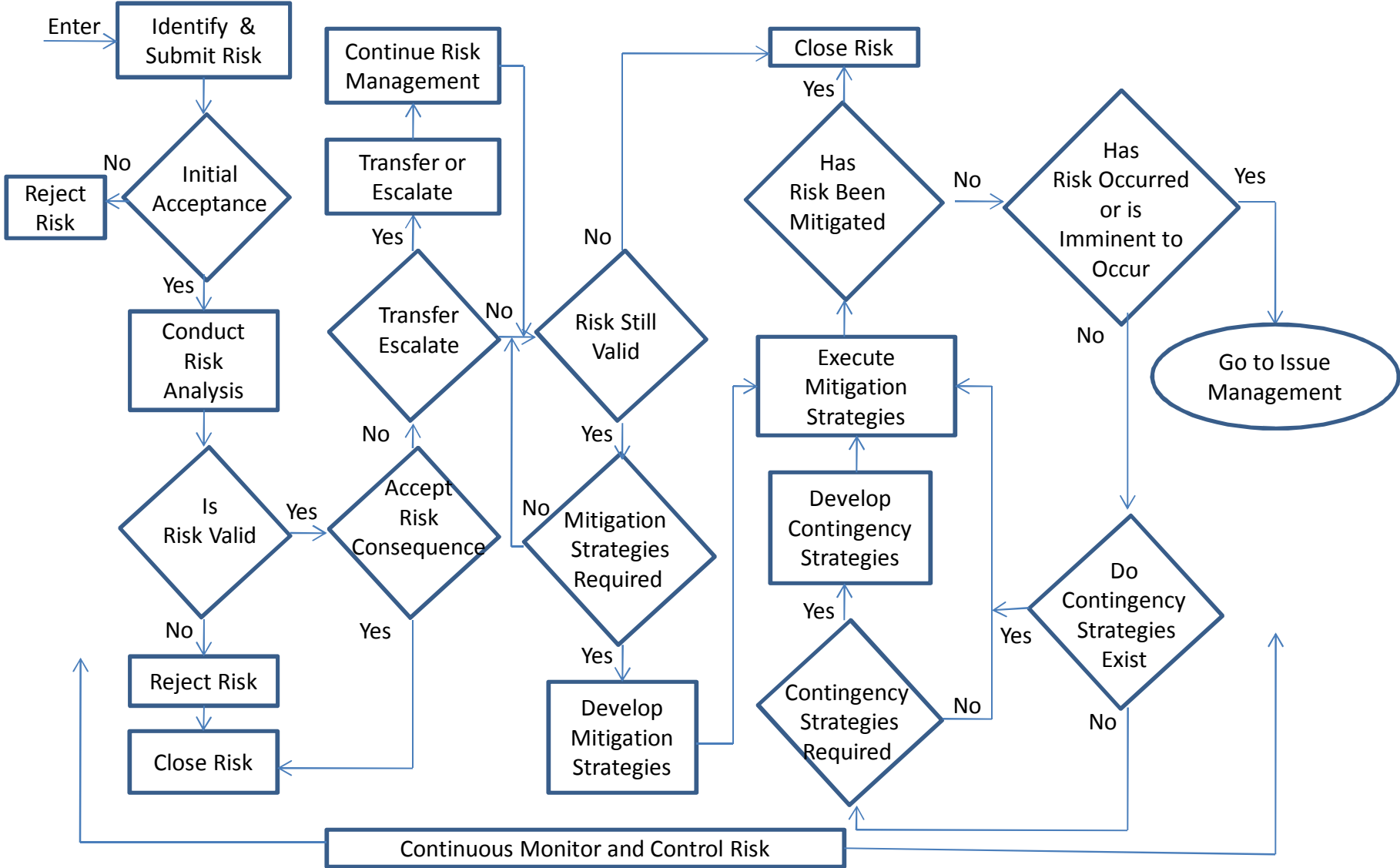
- The following are important guidelines for effective risk mitigation:
  - Prepare detailed mitigation strategies for all medium, high and very high risks
    - With sufficient detail about what is to be done, when, where, and by whom
  - Develop mitigation strategies as early as possible, allowing 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 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 Management Flow (In Review)



# Where Are We

- Introduction
- Risk Management

- { • ***References***
- ***Contact Information***



# 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®) v1.3*
  - *CMMI for Development*
  - *CMMI for Acquisition*
  - *CMMI for Service*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
- *Managing Risks, Methods for Software Systems Development*;  
Dr. Elaine M. Hall, SEI Series in Software Engineering
- [http://pascal.computer.org/sev\\_display/index.action](http://pascal.computer.org/sev_display/index.action) SEVOCAB:  
Software and Systems Engineering Vocabulary

# Contact Information



Alfred (AI) Florence  
[florence@mitre.org](mailto:florence@mitre.org)

Visit my transfer folder for this and other presentations including a half day tutorial on Risk Management