Definition of Risk

- Risk is the possibility of suffering loss, injury, disadvantage, or destruction.
  - [Webster's Third New International Dictionary 1981]

Risk Characteristics

- **Uncertainty**
  - a risk may or may not happen. There is some probability of it occurring
  - If it is inevitable, it is not a risk
- **Loss**
  - a risk has unwanted consequences
  - If there is no impact, its not a risk

Some Risk Wisdom

- Be a good risk manager or you will become a good crisis manager (SITC)
- If you don't actively attack the risks, they will actively attack you. (Tom Gilb)
- Projects that don't manage risk are at risk (ICE Corp)
- Risk management is not free; prepare to commit resources, define a risk management process, and make a risk reserve available.
- Risk in itself is not bad; risk is essential to progress (Roger Van Scoy)

Risk Management Goals

- Risks are systematically identified, analyzed, quantified, tracked and mitigated

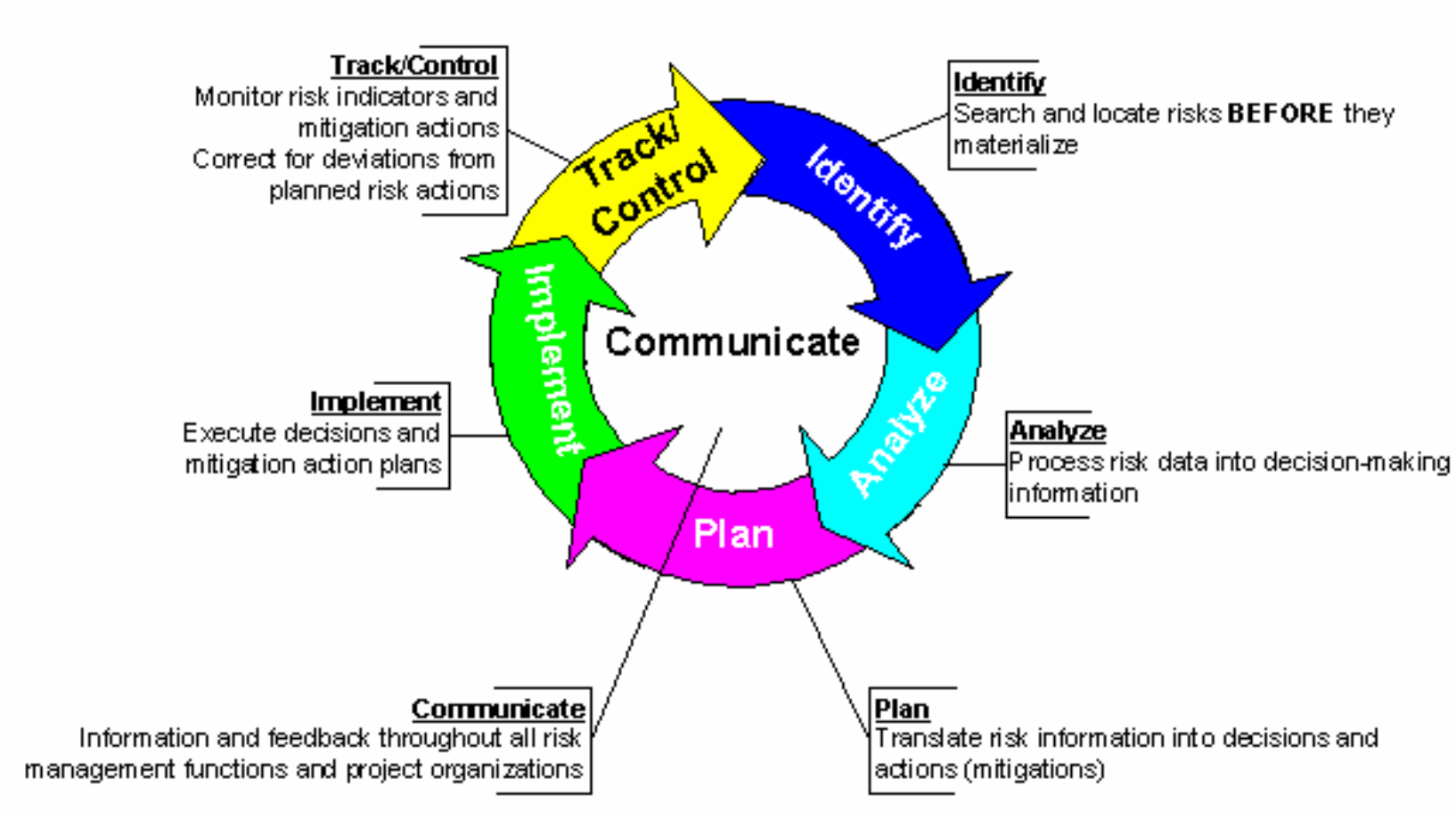
- Risk management information is used to make organizational and process improvements aimed at anticipating and eliminating all the causes of risk

Risk Management for CSE Systems

- **Risk Management Plan**
  - Assign responsibility for Risk Management
  - Identify risks
  - Analyze, measure, and prioritize risks
  - Mitigate risks and measure effect of the mitigation
  - Repeat process

Risk Management for CSE Systems

SEI Software Risk Management Process



Risk Identification : Activities

- **Discovery**
  - Historical data, experience, risk taxonomy, call for risks, brainstorming, risk indicators
- **Grouping**
  - Eliminate redundant risks; Combine related risks; Link dependent risks
  - Schedule/budget, new technology/obsolescence, etc.

Risk Indicators

- Unknown resources
- Lack of experience
- Lack of Information
- Complexity
- Lack of control
- Instability

Software Engineering Institute Risk Taxonomy

Risk Management for CSE Systems

A. PRODUCT ENGINEERING	
1. REQUIREMENTS	**3. CODE AND UNIT TEST**
A. Stability	A. Feasibility
B. Completeness	B. Testing
C. Clarity	C. Coding/Implementation
D. Validity	**4. INTEGRATION AND TEST**
E. Feasibility	A. Environment
F. Precedent	B. Product
G. Scale	C. System
2. DESIGN	**5. ENGINEERING SPECIALTIES**
A. Functionality	A. Maintainability
B. Difficulty	B. Reliability
C. Interfaces	C. Safety
D. Performance	D. Security
E. Testability	E. Human Factors
F. Hardware Constraints	F. Specifications
G. Non-Developmental Software	

Risk Management for CSE Systems

B. DEVELOPMENT ENVIRONMENT	
1. DEVELOPMENT PROCESS	**3. MANAGEMENT PROCESS**
A. Formality	A. Planning
B. Suitability	B. Project Organization
C. Process Control	C. Management Experience
D. Familiarity	D. Program Interfaces
E. Product control	**4. MANAGEMENT METHODS**
2. DEVELOPMENT SYSTEM	A. Monitoring
A. Capacity	B. Personnel Management
B. Suitability	C. Quality Assurance
C. Usability	D. Configuration Management
D. Familiarity	**5. WORK ENVIRONMENT**
E. Reliability	A. Quality Attitude
F. System Support	B. Cooperation
G. Deliverability	C. Communication
	D. Morale

Risk Management for CSE Systems

C. PROGRAM CONSTRAINTS	
1. RESOURCES	**3. PROGRAM INTERFACES**
A. Schedule	A. Customer
B. Staff	B. Associate Contractors
C. Budget	C. Subcontractors
D. Facilities	D. Prime Contractor
2. CONTRACT	E. Corporate Management
A. Type Of Contract	F. Vendors
B. Restrictions	G. Politics
C. Dependencies	

SEI Taxonomy-Based Questionnaire Sample

C. Program Constraints

1. Resources

A. Schedule (Is the schedule inadequate or unstable?)

- Is the estimation based on historical data?
- Has the method worked well in the past?
- Is there anything for which adequate schedule was not planned?

Risk Management for CSE Systems

Most Common MIS Risks	Occurrence
Creeping user requirements	80%
Excessive schedule pressure	65%
Low quality	60%
Cost Overruns	55%
Inadequate Configuration Control	50%

From Jones, Capers. *Assessment and Control of Software Risks*. Englewood Cliffs, N.J.: PTR Prentice-Hall, 1994

Some Observed CSE System Problems / Risks

- Lack of continuity in staff
- Lack of executive commitment
- Lack of cooperation between State agencies
- Inadequate or intermittent funding
- Intermittent development efforts
- Poorly understood legacy systems
- Contractor non-performance
- Many external interfaces / Poorly defined external interfaces

Risk Management for CSE Systems

Some More Observed CSE System Problems / Risks

- Lack of domain expertise
- Management review/decision cycle is slower than expected
- Non-technical third-party tasks take longer than expected (budget approval, equipment purchase approval, legal reviews, etc.)
- Lack of accurate status reporting
- Lack of user input
- Requirements are poorly defined and unstable
- Lack of quantitative historical data

Risk Analysis: Activities

- **Grouping**
  - Eliminate redundant risks; Combine related risks; Link dependent risks
  - One possible grouping - Organizational, Process, Product
  - Schedule/budget, new technology/obsolescence, etc.

- **Quantification**
  - Establish Measurement scale
  - Measure probability, consequence, time frame
  - Risk Exposure = Likelihood x Consequence

- **Ranking**
  - Order of likelihood, consequence, exposure, time frame

- **Identifying Triggers**
  - Define scenarios or conditions that indicate occurrence of a risk is imminent

Quantifying Consequence

Magnitude	Capability Factor	P.R. Factor	Cost Factor	Schedule Factor
0.1 Low	Minimal or no consequences, unimportant	Occasional harsh write-ups in newspapers	Budget estimates not exceeded	Negligible impact on implementation schedules
0.3 Minor	Small reduction in capability	Called before legislature or investigative body	Cost estimate exceeds budget by 1 to 5%	Minor slip in schedules (less than 1 month), small adjustments in milestones required
0.5 Moderate	Some reduction in capability	Unfavorable public opinion	Cost estimate exceeds budget by 5 to 20%	Schedules slip up to 3 months
0.7 Significant	Significant capabilities missing	Severe pressure to replace key officials	Cost estimate exceeds budget by 20 to 50%	Schedules slip up to 6 months
0.9 Catastrophic	Technical goals cannot be achieved	Budget cuts as political retribution	Cost estimate exceeds budget by >50%	Schedules slip more than 6 months

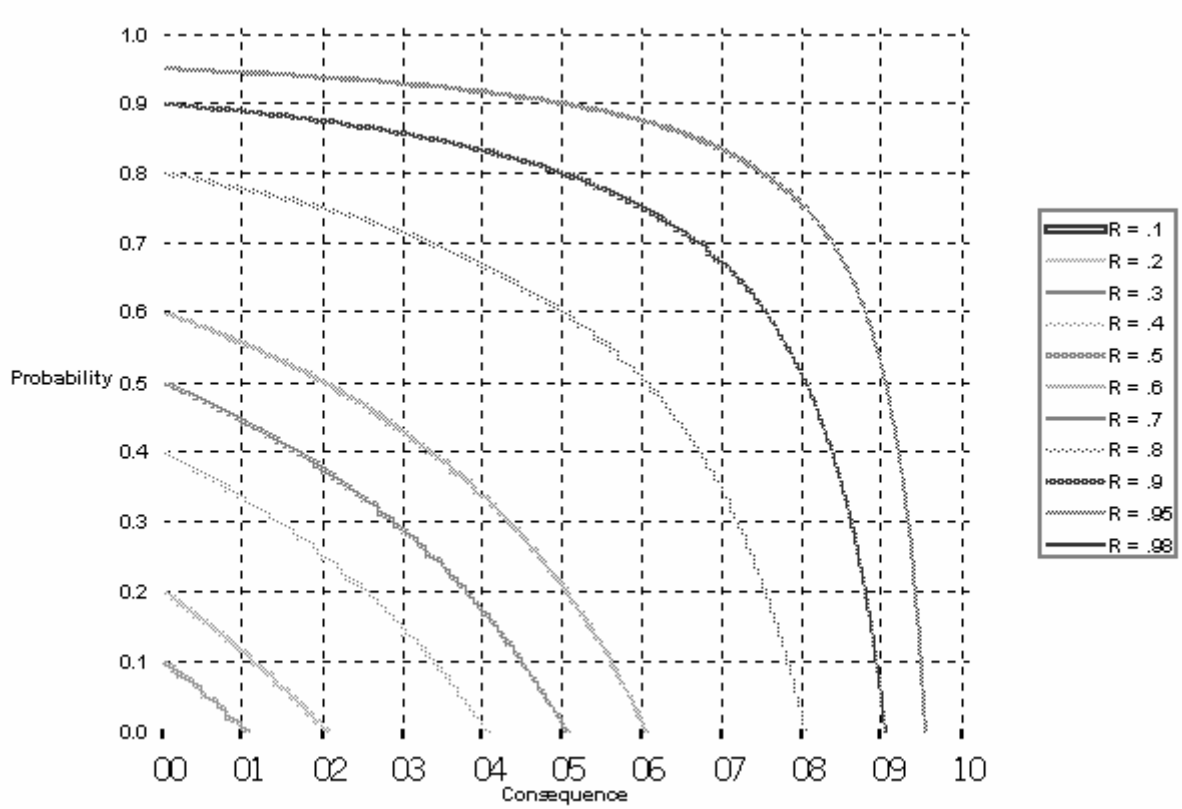
Quantifying Probability

	Maturity Factor	Complexity Factor	Dependency Factor	Stability Factor
0.1 Low	Technology exists and can be used "as is"	Simple relative to current environment	Entirely within project control	External factors will not make any changes
0.3 Moderate	Technology requires minor change before use (<25%)	Minor complexity relative to current environment	Depends on existing product supplied from outside organization	External factors will make minor changes (<25%)
0.5 High	Technology requires major change before use (<50%)	Moderately complex relative to current environment	Depends on supply and modification of existing product from outside organization	External factors will make major changes (<50%)
0.7 Very High	Technology requires significant design and engineering before use (<75%)	Significantly complex relative to current environment	Depends on new development from outside organization	External factors will make significant changes (<75%)
0.9 Extremely High	State of the art, some research done	Extremely complex relative to current environment	Depends on finding development from outside organization	External factors will make constant changes

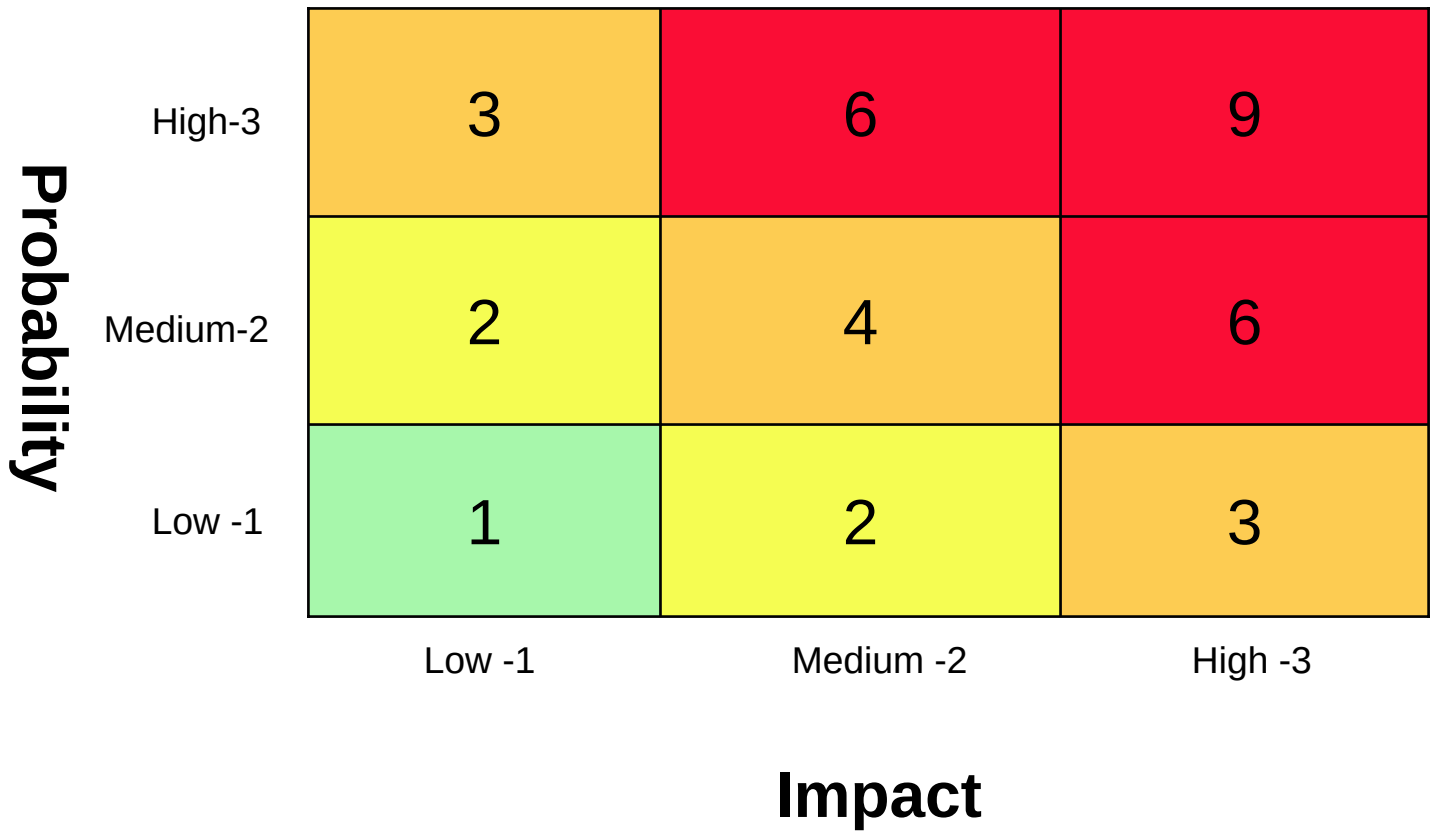
Risk Management for CSE Systems

Generic Software Project Risk Factors						
Risk Factors	***Low Risk Cues***	***Medium Risk Cues***	***High Risk Cues***	**L**	**M**	**H**
Project Team						
Team Member Availability	in place, little turnover expected; few interrupts for fire fighting	available, some turnover expected; some fire fighting	high turnover, not available; team spends most of time fighting fires			
Application Experience	extensive experience in team with projects like this	some experience with similar projects	little or no experience with similar projects			
Experience with Process	extensive experience with this process	some experience with this process or extensive experience with another	little or no experience with a defined process			
Training of Team	training plan in place, training ongoing	training for some areas not available or training planned for future	no training plan or training not readily available			

Iso-Risk Contour Chart



Simple Risk Exposure Chart



Risk Mitigation

- Prioritize risks by triggers, exposure and timeframe. Deal with the most critical first.
- All non-negligible risks must have mitigation strategies.
  - Obtain more information as necessary to eliminate or reduce uncertainty
  - Document decisions and strategies

Risk Mitigation : Activities

- **Risk Reduction**
  - Take action to reduce risk -hold training, add resources, reduce scope of project, etc.
- **Risk Contingency**
  - Have resources (money, staff, equipment, etc.) available to handle occurrence of risk
- **Risk Transfer**
  - Get someone else to accept the risk – not recommended – if done, keep tracking the risk
- **Risk Acceptance**
  - Live with it – appropriate only for low consequence risks

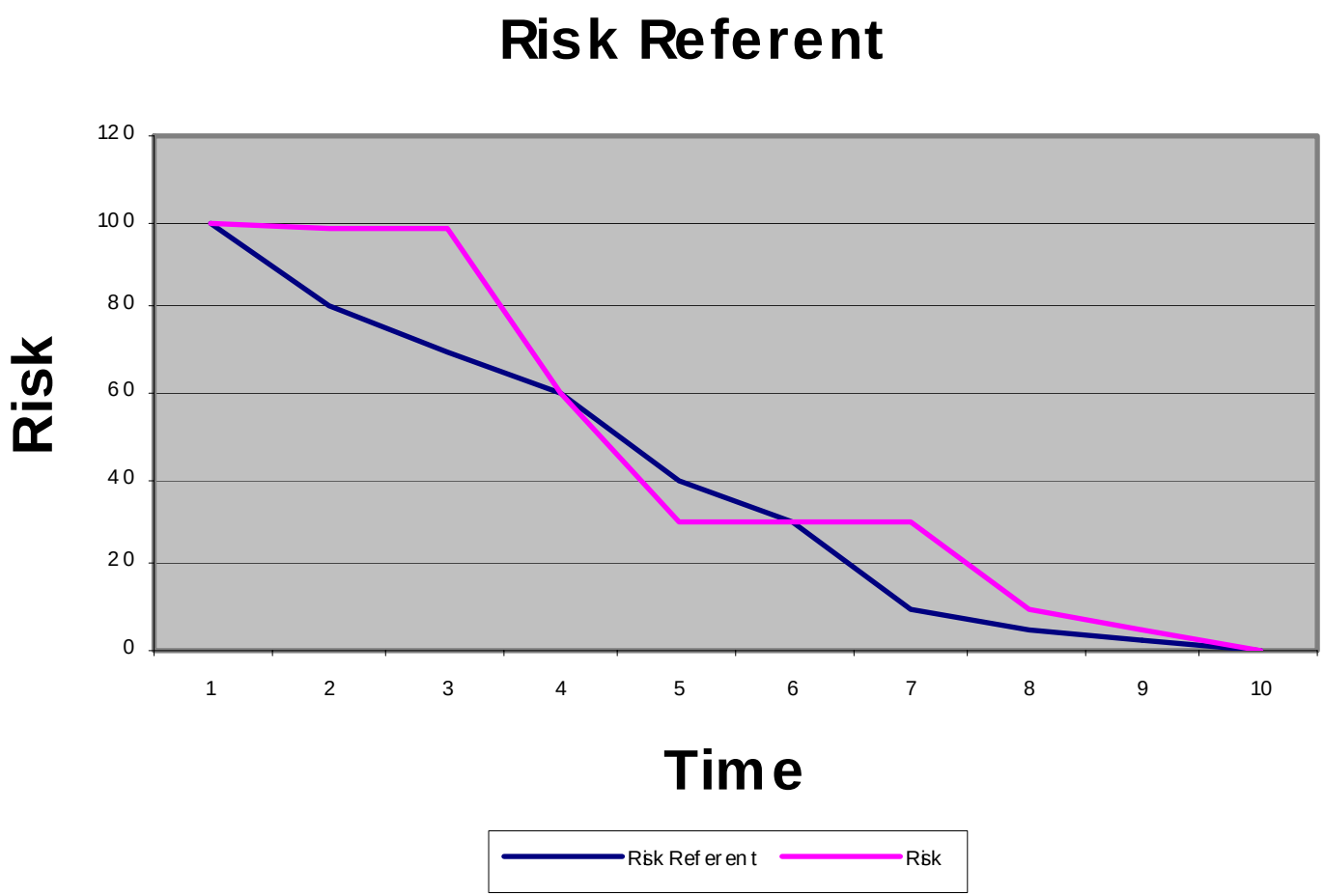
Risk Management for CSE Systems

Risk	Mitigation
Creeping user requirements	Requirements elicitation - consult stakeholders early, plan for requirements growth (10% per month)
Excessive schedule pressure	Planning (7% of system cost), cost estimation, communications
Low quality	Planning (Quality Assurance Plan), independent QA organization, training, IV&V
Cost Overruns	Cost estimation, planning
Inadequate Configuration Control	Planning (Configuration Management Plan), Training, Automated CM tools

Risk Tracking : Activities

- **Monitor risk triggers**
  - Watch for signs of a risk occurring – give early warning
- **Monitor overall project risk (Risk Referent)**
  - Is the total risk (sum of all risk exposure) decreasing as expected ?
- **Notify stakeholders**
  - Let stakeholders know the risk is happening
- **Collect information on all risks**
  - Update risk database

Risk Management for CSE Systems



Risk Tracking Form

RISK ID	Risk Information Sheet		Date Identified:
Priority	Risk Statement		
Probability			
Impact			
Timeframe	Originator	Classification	Assigned to:
Context			
Approach: Research / Accept / Watch / Mitigate			
Contingency Plan and Trigger			
Status			Date_____
Lessons Learned			
Approval	Closing Date	Closing Rationale	

Risk Management for CSE Systems

- **Do frequently occurring project risks point to a underlying process weakness?**
- **Does your organization's current process capability suggest inherent risks for all projects?**

Turn Risk Management into Process Improvement !

Risk Management for CSE Systems

Risk Management → Process Improvement

Seeks to avoid or minimize impact to project success	Seek permanent change in practices and infrastructure
Project activity	Organizational-wide effort
Get-well quick	Multi-year initiative
Short-term relief	Long-term measurable benefits

What Is Needed For Risk Management To Work?

- **Risk Management Policy and Commitment -** Establishes the framework that enables Risk Management to work
- **Risk Management Coordinator -** Someone with authority to plan, implement and support the Risk Management process
- **Risk Management Plan -** Defines the Risk Management processes and roles and responsibilities.
- **Continuous Independent Risk Assessment -** ongoing, unbiased evaluation of project's cost, schedule, technical and performance risks
- **Risk Management Database** – A place to store, analyze, prioritize, report and monitor risk data throughout the project life cycle

Links

Software Engineering Institute
http://www.sei.cmu.edu

National Human Services IT Resource Center
http://www.acf.hhs.gov/nhsitrc/

Texas Department of Information Resources
http://www.dir.state.tx.us/eod/qa/risk/index.htm