RISK MANAGMENT

- Four activities for risk management:
  - **Risk Identification:** list down all risks
  - **Risk Analysis:** probability of the listed risks occuring
  - **Risk Analysis:** damage of each risk
  - **Risk Mitigation:** reducing impact of the risk after occurence
- Some **general risks** in project:
  - Cost estimation for project; underestimation
  - Problem in scheduling
  - Absence of relevance or technical staff (downsizing)
  - Lack of resources
  - Ambiguity in requirements
- Also measure the impact of these risks

- Plan referes to mitigation
- This cycle continues as new risks are being identified as project continues.
- **Risk management strategies:**
  - **Reactive:** wait for risk and then take measures to handle
  - **Proactive:** manage and take measures before risk occurs
- Each of them has equal adv. and disadv. such as taking too much proactive measures could cause los of budgeting and resources if they were spent to avoid the risk but it never occurred
- **Types of Risks:**
  - **Technical:**
    These include:
    - **Design risks:** concerns the architecture of our software and whether we have the resources to complete it

- **Implementation risks:** relevant tools, hardware, or staff available to undertake the project
- **Interface risks:** concerns both human and component interface, such as unable to make an interactive GUI or unable to get API for a component
- **Verification risks:** system not verified properly or test-cases not effective
- **Maintenance risks:** downsizing may cause staff changes and hence potential maintenance issues
- **Ambigous requirements, technology becoming obselete, technology new** so less resources hence more uncertainity in problems.

- **Business Risks:**
  - **Market Risk:** excellent product but not needed in market (improper market analysis)
  - **Strategic Risk:** technology market changing hence product does not fit business strategy (e.g nokia)
  - **Sales risk:** sales force unable to sell product due to less knowledge. More domain knowledeg will lead to better sales
  - **Management risk:** change in senior management will cause change in policies hence will affect product
  - **Budget Risks:** some activities such as QA analysis etc. may not be performed due to loss of budget hence affecting product
- **Known risks:**
  - Those that can be resolved after careful evaluation of project plan, business environments etc such as lack of documentation, poor dev environment, unrealisitic delivery date
- **Predictable risks:**
  - Risks that can be predicted from similar past experiences of projects such as predicting staff turnover, poor communication with customer etc.
- **Unpredictable risks:**
  - Unforseen risks such as natural calamity, lockdowns etc.
- **General risks:**

        - Risks common to all products of the same domain hence when occur may affect all projects such as:
            - Staff turnover
            - Budget problems
    - **Product specific risk:**
        - Occur and affect only specific projects such as resource requirement for a certain project etc.
- **Risk identification generic checklist:**
  Mostly occuring risks (some are general and some are product specific):
    - **Product size (PS):** software size may exceed expected due to increasing lines of code, or dependencies involved etc.
    - **Business impact (BU):** 5 business risks discussed above, competitor launches same product but better imposing risk on your product
    - **Stakeholder characteristics (SC): mostly occuring risk!** Problems in requirements engineering, sophistication in communication with stakeholder in timely manner
    - **Process definition (PD):** random development of software, without priority setting or roadmap for development such as agile will put your quality at risk
    - **Development environment (DE):** unavailibility of tools / resources to build software
    - **Technology to be built (TE):** risk regarding complexity of system, technology obselete or ‘newness’ of technology
    - **Staff size and experience (ST):** risk regarding technical and project related experience of the staff
- Question discussed in next slide:
    - 1-5: Stake holder characteristics
        1. Is senior management supporting project? Necessary for imposing software development on lower management
        2. Are end users showing interest for software? May cause ambiguity in software development
        3. – 5. Pertaining requirements specficiation of project
    - 6-11: all scheduling and staff related risks
- **Risk Drivers:**
    - Software risks to be analyzed at managerial level:

    - Performance: uncertainity of that project able to achieve goal and deliver as required
    - Cost: uncertainity of project budget
    - Support: uncertainity that software is flexible, adaptable, easy-use, not too rigid that doesn't allow correction
    - Schedule: uncertainity that schedule will be maintained and product will complete on time
- **Risk Estimation:**
    - Probability of risk and then measuring the severity of consequences for that risk
- **Risk Impact:**

  Risk's impact can be categorized as:
    - Negligible: this won't cause inconveniencies, or problems even if occured
    - Marginal: objective target is still achievable and deadlines are still realistic as failures are small, can be handled during development
    - Critical: cause problems to some but major features
    - Catastrophic: cause problems to whole system

Category \ Components		Performance	Support	Cost	Schedule
Catastrophic	1	Failure to meet the requirement would result in mission failure		Failure results in increased costs and schedule delays with expected values in excess of $500K	
	2	Significant degradation to nonachievement of technical performance	Nonresponsive or unsupportable software	Significant financial shortages, budget overrun likely	Unachievable IOC
Critical	1	Failure to meet the requirement would degrade system performance to a point where mission success is questionable		Failure results in operational delays and/or increased costs with expected value of $100K to $500K	
	2	Some reduction in technical performance	Minor delays in software modifications	Some shortage of financial resources, possible overruns	Possible slippage in IOC
Marginal	1	Failure to meet the requirement would result in degradation of secondary mission		Costs, impacts, and/or recoverable schedule slips with expected value of $1K to $100K	
	2	Minimal to small reduction in technical performance	Responsive software support	Sufficient financial resources	Realistic, achievable schedule
Negligible	1	Failure to meet the requirement would create inconvenience or nonoperational impact		Error results in minor cost and/or schedule impact with expected value of less than $1K	
	2	No reduction in technical performance	Easily supportable software	Possible budget underrun	Early achievable IOC

Note: (1) The potential consequence of undetected software errors or faults.
(2) The potential consequence if the desired outcome is not achieved.

Risks	Category	Probability	Impact	RMMM
Size estimate may be significantly low	PS	60%	2	
Larger number of users than planned	PS	30%	3	
Less reuse than planned	PS	70%	2	
End-users resist system	BU	40%	3	
Delivery deadline will be tightened	BU	50%	2	
Funding will be lost	CU	40%	1	
Customer will change requirements	PS	80%	2	
Technology will not meet expectations	TE	30%	1	
Lack of training on tools	DE	80%	3	
Staff inexperienced	ST	30%	2	
Staff turnover will be high	ST	60%	2	
Σ				
Σ				
Σ				

Impact values:
1—catastrophic
2—critical
3—marginal
4—negligible

- **Risk Impact Assessment:**
  - **Risk exposure = Probability of risk x Cost if risk occurs**
  - **LOC =** line of code
- **Risk Mitigation:**
  - Determine the causes for the risk
  - Mitigate those causes if under your control
  - Have a backup plan in case something goes wrong
  - E.g employee turnover (refer to slides)
- **Risk contigency:**
  - Steps to be taken to reduce risk impact even after all mitigation efforts

Table 4: Sample Student Risk Table

Rank	Risk	Probability	Impact	Rank Last Week/ Weeks on list	Action
1	None of us knows how to use the technology.	frequent	critical	1/5	Read. Do tutorials.
2	Integration problems.	frequent	critical	2/5	Integrate all work Sunday nights.
3	Someone drops the class.	improb	critical	4/5	Pair programming for all work.
4	Team members missing important team meetings.	improb.	marginal	5/4	Person who misses meeting has to supply Sunday night pizza the next week.
5	Overriding each other's work	improb	marginal	3/5	Continue using CVS.

- **Risk Information sheet:**
- This involves the proactive approach. Hence, we define context in which the risk may occur such as taking help from 3rd party APIs etc. Then we define mitigation steps that could be taken along with a contigency plan in-case something goes wrong. A sample can be seen below:

Risk information sheet

Risk ID: P02-4-32	Date: 5/9/09	Prob: 80%	Impact: high

Description:
Only 70 percent of the software components scheduled for reuse will, in fact, be integrated into the application. The remaining functionality will have to be custom developed.

Refinement/context:
Subcondition 1: Certain reusable components were developed by a third party with no knowledge of internal design standards.
Subcondition 2: The design standard for component interfaces has not been solidified and may not conform to certain existing reusable components.
Subcondition 3: Certain reusable components have been implemented in a language that is not supported on the target environment.

Mitigation/monitoring:
1. Contact third party to determine conformance with design standards.
2. Press for interface standards completion; consider component structure when deciding on interface protocol.
3. Check to determine number of components in subcondition 3 category; check to determine if language support can be acquired.

Management/contingency plan/trigger:
RE computed to be $20,200. Allocate this amount within project contingency cost. Develop revised schedule assuming that 18 additional components will have to be custom built; allocate staff accordingly.
Trigger: Mitigation steps unproductive as of 7/1/09.

Current status:
5/12/09: Mitigation steps initiated.

Originator: D. Gagne	Assigned: B. Laster

Some general risk:

Boehm's prioritized top-ten list of software risk items:

Risk item	Risk Management techniques
1. Personnel shortfalls	Staffing with top talent, job matching; teambuilding; cross-training; pre-scheduling; key people; morale building
2. Unrealistic schedules and budgets	Detailed, multisource cost and schedule estimation; design to cost; incremental development; software reuse; requirements scrubbing
3. Developing the wrong software functions	Organization analysis; mission analysis; ops-concept formulation; user surveys; prototyping; early users' manuals
4. Developing the wrong user interface	Task analysis; prototyping; scenarios; user characterization (functionality, style, workload)
5. Gold plating	Requirements scrubbing; prototyping; cost-benefit analysis; design to cost
6. Continuing stream of requirement changes	High change threshold; information hiding; incremental development (defer changes to later increments)
7. Shortfalls in externally furnished components	Benchmarking; inspections; reference checking; compatibility analysis
8. Shortfalls in externally performed tasks	Reference checking; pre-award audits; award-fee contracts; competitive design or prototyping; teambuilding
9. Real-time performance shortfalls	Simulation; benchmarking; modeling; prototyping ;instrumentation; tuning
10. Straining computer-science capabilities	Technical analysis; cost-benefit analysis; prototyping; reference checking

- Lack of employees
- Unrealistic deadline and estimated plans
- Goldplating: providing user with unecessary exaggerations in software instead of giving required functionality. Such as providing a very interactive UI with little or no backend which was the main part!