

An Effective Risk Management Tool - Software Risk Checklist

Muhammad Mahbub Hussain

**Post Graduate Student, School of Computing and Information Technology (SCIT)
University of Western Sydney (Paramatta Campus)**

This document basically presents a Software Risk Checklist. This checklist is only an aid to start the managers and engineers thinking and planning how to realize, avoid, mitigate and accept the risks inherent in any software project. It is laid out by development phases of a project, concentrating on the software lifecycle portion of the overall project lifecycle. Listed here are some (not an exhaustive list) of the generic risks that should be considered when any project contains software development. The project manager, software manager, system engineer/manager, any software technical leads, and the software engineers, as a minimum, should review, fill out and discuss the results of this checklist. Taking into account all the different perspectives and adding risks specific to a project, the review team should then meet to create an agreed upon set of risks and start planning how they will be addressed.

This checklist covers number of lifecycle stages/phases. A first-pass review of the entire checklist may be helpful during systems requirements in order to help create the initial list of identified risks. These risks should be recorded in a database or series of mitigation plans. Once the risk list, database, mitigation plan, and/or management plan have been established, it is suggested that the applicable section of this checklist be reviewed again at the beginning of each subsequent, applicable lifecycle phase in order to add additional risks or modify current ones. If the project is using rapid prototyping or the spiral lifecycle, then periodic revisiting of this checklist should be established and followed. The software management plan would be a good place to document this process.

The checklist is laid out with the generic risks listed followed by a column to indicate if this is a risk for a particular project. **(Y)**es, this is a risk; **(N)**o, not a risk for this project at this time; **(P)**artially a problem as stated, further clarification should be added. The last column is to indicate if this risk should be accepted or needs to be worked, i.e. added to a risk mitigation plan with action items or task plans to track risks to closure. For details on mitigation plans, the *SEI Continuous Risk Management Guidebook* can be viewed/ referred.

The "Software Risk Checklist" is presented from the next page until the end of this document.

Project Development Phase:	RISK Yes/No /Partial	ACTION Accept/W ork
System Requirements Phase		
Are system level requirements documented? To what level? Are they clear, unambiguous, verifiable?		
Is there a project wide method for dealing with future requirements changes?		
Have software requirements been clearly delineated/allocated?		
Have these system level software requirements been reviewed, inspected with systems, hardware and the users to insure clarity and completeness?		
Has Firmware and Software been differentiated, who is in charge of what and is there good coordination if H/W is doing "F/W"?		
Are the effects on command latency and its ramifications on controllability known?		
Can the Bus bandwidth support projected data packet transfers?		
Are requirements defined for loss of power? System reaction known or planned for? UPS (Un-interruptible Power Supplies) planned for critical components?		
Is an impact analysis conducted for all changes to baseline requirements		

Software Planning Phase	<u>RISK</u>	<u>ACTION</u>
Is there clarity of desired end product? Customer & builders (system and software) agree on what is to be built and what software's role is?		
Are system level requirements on Software documented? and are they complete/sufficient and clearly understood		
Are all interface requirements known & understood?		
Roles and responsibilities for system & software clearly defined and followed and sufficient		
Have the end user/operator requirements been represented in the conception phase such that their requirements are flowed into the software requirements?		
Has all needed equipment, including spares been laid out? and ordered? Is there sufficient lead time to get needed equipment? Is there a contingency plan for not getting all equipment? Is there a contingency plan for not getting all equipment when needed?		
Is the needed level of technical expertise known?		
Level of expertise available: From contractors? Will expertise be available as the schedule demands? Is there more than one person with a particular expertise/knowledge?		
Training: Enough trained personnel? Time to train all personnel? on project ? on equipment/ software development environment, etc.? Time and resources to train additional personnel as needed?		
Budget: Is budget sufficient for: equipment needed personnel training travel etc.		

Schedule Is Schedule reasonable considering needed personnel, training and equipment? Does system level schedule accommodate software lifecycle? Can necessary equipments be made available in time?		
Has all the slack/contingency time on the critical path been used up?		
Are software metrics kept and reported regularly? Monthly?		
Are deviations to the development plan being tracked? Trended? Are the trends reported in a manner to allow timely and appropriate software and project management decisions?		
Will new development techniques be used?		
Will new or different development environment be used?		
Is this a new technology?		
Will simulators need to be designed and built? Is there time and resources allocated for this?		
Is there a schedule for development of ground and flight software? Is it reasonable, does it match reality? Is it being followed? Are changes tracked and the reasons for the changes well understood?		
Do the schedules for ground and flight software match up with what is needed for test and delivery?		
Will test software need to be designed and developed? Is there time and resources allocated for this?		
Distributed development environment: Will this be a distributed development (different groups or individuals working on parts of the project in different locations e.g. out of state)? Are there proper facilities and management structure to support distributed development?		
Inter/Intra group Management Are interfaces with other developers, suppliers, users, management, customer understood and documented? Is there a known way to resolve differences between these groups (i.e. conflict resolution/ who has ultimate authority, who is willing to make a decision)?		
Management Planning: Is management experienced at managing this size and/or type of team (Experienced Project Manager?)? Is management familiar with the technology being used (e.g. OOA/OOD and C++)? Is there a well constructed software management plan that outlines procedures, deliverables, risk, lifecycle, budget, etc. Is it reasonable, does it match reality? Is it being followed?		
Does software lifecycle approach & time-frame meet needs of overall project, does it have a chance of being close to what is needed?		
Has time been allocated for safety, reliability and QA input and auditing		
Have software development standards & processes been chosen?		
Have software documentation standards been chosen?		
Has Software Product Assurance had input on all standards, procedures, guidelines & processes?		
Is funding likely to change from originally projected? Is there a plan in place to handle possible funding changes? Prioritization of requirements?		

Phasing of requirements delivery?		
Is there a procedure/process for handling changes in requirements?		
Is it sufficient?		

Software Requirements Phase	RISK	ACTION
<p>Software Schedule:</p> <p>Is there an adequate software Schedule in place? Is it being followed? Are changes to schedule being tracked?</p> <p>Are changes to schedule made by due process, in a planned manner or are events changing the schedule with no decision of whether there is something wrong in the process or program that needs to change to make schedule?</p> <p>Has it been chosen to meet the needs of software development or is just a time/date when systems will need the software?</p>		
Has all the slack/contingency time on the critical path been used up?		
Are software metrics kept and reported regularly? Monthly?		
Are deviations to the development plan being tracked? Trended? Are the trends reported in a manner to allow timely and appropriate software and project management decisions?		
Are parent documents baselined before child documents are reviewed? Is there a process in place for assessing the impact of changes to parent documents on child documents? Is there a process in place for assessing the impact of changes to parent documents from changes within child documents?		
Are review/inspection activities and schedules well defined and coordinated with sufficient lead time for reviewers to review material prior to reviews/inspections?		
Is there a process for closing out all TBDs before their uncertainty can adversely affect the progress of the project?		
<p>Has the Project planned how to handle changing requirements?</p> <p>Compartmentalized design? Procedures/ change boards in place for accepting/rejecting proposed changes? Includes how schedule impacts are dealt with? Is the project following these procedures? Is there good communication with the Principle Investigators/Customer? Have requirements been prioritized? Is this prioritization tracked, reviewed and periodically updated? Is there a clear understanding of what is really necessary for this project?</p>		
Have there been changes/reductions in personnel since first estimates?		
<p>Are there sufficient trained software personnel? Does all the knowledge for any aspect of project reside in just one individual?</p>		
<p>Are the requirements, both from the system level and those levied by standards, chosen? Have guidelines, etc. been established?</p>		
Is there a Software Testing/Verification Plan?		
<p>Is the Software Management Plan being followed? Does it need to be adjusted?</p>		
Is the software development environment chosen and in place?		

Any work contracted out has sufficient controls and detail to assure quality, schedule, and meeting of requirements?		
Software Configuration Management Plan in place and working?		
Are backups of SCM system/database planned and carried out on a regular basis?		
Are Inspections or peer reviews scheduled and taking place?		
Software Quality/Product Assurance (SQA or SPA): Is SPA working with development to incorporate Safety, Reliability and QA requirements? Is s/w development working with SPA to help establish Software Processes? Does SPA have a Software Auditing Process and Plan in place?		
Are there good lines of communication established and working between software project groups?		
Good lines of communication established and working with groups outside software development? Are there written agreements on how to communicate? Are they followed? Are they supported by management and systems group? Are there good interface documents detailing what is expected? Did all the concerned parties have a chance to review and agree to them?		

<p>Have resources been re-evaluated (equipment, personnel, training, etc.) Are they still sufficient? If not, what measures are taking place to adjust project schedule, budget, deliverables, etc. (more personnel, reprioritization and reduction of requirements, order new equipment, follow previously established mitigation plan, etc.)?</p>		
<p>Are COTS being used? How are COTS maintained? Who owns them, who update them? How is product affected by changes to COTS? New releases of one or more COTS, how will they be maintained/supported? How will COTS releases be coordinated with the developed software maintenance and releases? Do COTS meet the necessary delivery schedule? Do personnel have a good understanding of how to use/integrate COTS into final product?</p> <p>If COTS meet only a subset of requirements, has the integration task and time been correctly estimated? Can it be estimated?</p> <p>Will custom software need to be written to either get different COTS to interact or to interact with the rest of the system as built or planned?</p>		
<p>Is a new technology/methodology being incorporated into software development? Analysis? Design? Implementation? (e.g. Formal Methods, OOA, etc.) Has the impact on schedule, budget, training, personnel, and current processes been assessed and weighed? Is there process change management in place?</p>		
<p>Is a new technology being considered for the system? Has the impact on schedule, budget, training, personnel, and current processes been assessed and weighed? Is there process change management in place?</p>		
<p>Is the project planning to do prototyping of unknown/uncertain areas of project to find requirements, equipment and/or design criteria that may not be able to be met in way originally planned.</p>		

Software Design Phase	RISK	ACTION
Is the Software Management Plan being followed? Does it need updating?		
Is the Requirements flow down well understood?		
Standards and guidelines sufficient to produce clear, consistent design and code?		
Will there be, has there been, a major loss of personnel (or loss of critical personnel)?		
Communication between systems and other groups (avionics, fluids, operations, ground software, testing, QA, etc.) and Software working well both directions?		
Requirements Have they been baselined & are they configuration managed? Is it known who is in charge of them? Is there a clear, traced, managed way to implement changes to the requirements? (i.e. is there a mechanism for in-putting new requirements, or altering old, established and working)? Is there sufficient communication between those creating & maintaining requirements and those designing to them? Is there a traceability matrix between requirements and design? Does that traceability matrix show the link from requirements to design and then to the appropriate test procedures?		
Has System Safety assessed Software? Any software involved hazard reports? Does software have the S/W subsystem hazard analysis? Does software personnel know how to address safety critical functions, how to design to mitigate safety risk? Are there Fault Detection, Isolation and Recovery (FDIR) techniques designed for critical software functions?		
Has software reliability been designed for? What level of fault tolerance has been built in to various portions /functions of software?		
Need to create Simulators to test software? Were these simulators planned for in the schedule? Are there sufficient resources to create, verify and run these? How heavily does software completion rely on simulators? How valid (close to the flight) are the simulators?		

<p>Need to create Simulators to test hardware?</p> <p>Are these simulators accurate?</p> <p>Are they maintained up to date with changing Flight H/W?</p> <p>Were these simulators planned for in schedule?</p> <p>Are there sufficient resources to create, verify and run these?</p> <p>How heavily does hardware completion rely on simulators?</p>		
<p>Is firmware and/or any other software developed outside the software flight group?</p> <p>Is it being integrated?</p> <p>Is it being kept current based on changes to requirements & design?</p> <p>Is it configuration managed?</p>		
<p>Any work contracted out has sufficient controls and detail to assure quality, schedule and meeting of requirements?</p>		
<p>Will design interfaces match in-house or other contracted work?</p>		
<p>Software Configuration Management Plan in place and working?</p>		
<p>Are backups of SCM system/database planned and carried out on a regular basis?</p>		
<p>Are Inspections and/or peer reviews scheduled and taking place?</p>		
<p>Software Quality/Product Assurance (SQA or SPA):</p> <p>Is SPA working with development to incorporate Safety, Reliability and QA requirements into design?</p> <p>Does SPA have a Software Auditing Process and Plan in place?</p> <p>Have they been using it?</p>		
<p>Are parent documents baselined before child documents are reviewed?</p> <p>Is there a process in place for assessing the impact of changes to parent documents on child documents?</p> <p>Is there a process in place for assessing the impact of changes to parent documents from changes within child documents?</p>		
<p>Are review/inspection activities and schedules well defined and coordinated with sufficient lead time for reviewers to review material prior to reviews/inspections?</p>		
<p>Has all the slack/contingency time on the critical path been used up?</p>		
<p>Are software metrics kept and reported regularly? Monthly?</p>		
<p>Are deviations to the development plan being tracked? Trended?</p> <p>Are the trends reported in a manner to allow timely and appropriate software and project management decisions?</p>		

Software Implementation Phase	<u>RISK</u>	<u>ACTION</u>
Coding and unit test		
Is the software management plan still being used? Is it up to date?		
Are there coding standards?		
Are they being used?		
Software Development Folders (SDFs) being used to capture design and implementation ideas as well as unit test procedures & results?		
Code walk-throughs and/or inspections being used? Are they effective as implemented?		
SQA/SPA auditing development process and SDFs?		
Is design well understood and documented?		
Are requirements being flowed down through design properly?		
Is schedule being maintained? Have impacts been accounted for (technical, resources, etc.)? Is it still reasonable?		
Has all the slack/contingency time on the critical path been used up?		
Are software metrics kept and reported regularly? Monthly?		
Are deviations to the development plan being tracked? Trended? Are the trends reported in a manner to allow timely and appropriate software and project management decisions?		
Have any coding requirements for safety critical code been established? If so, are they being used?		
Does chosen development environment meet flight standards/needs?		
Has System Safety assessed Software (Subsystem Safety Analysis)? Has software reviewed this safety assessment? Has software had input to this safety assessment? Does software personnel know how to address safety critical functions? Is software working with systems to find the best solution to any hazards?		
Has FDIR (Fault Detection, Isolation and Recovery) and/or Fault Tolerance been left up to implementation (i.e. no hard requirements and/or no design for these)?		
Is there a known recourse/procedure for design changes? Is it understood? Is it used? Does it take into account changes to parent documents? Does it take into account subsequent changes to child documents?		

<p>Is there a known recourse/procedure for requirements changes? Is it understood? Is it used? Is it adequate, does it need to be altered? Does it take into account changes to parent documents? Does it take into account subsequent changes to child documents?</p>		
<p>Is there development level Software Configuration Management (SCM) (for tracking non-baseline changes and progress) Is it being used by all developers, regularly Are backups performed automatically on a regular basis?</p>		
<p>Is there formal SCM and Baselineing of Requirements and Design?</p>		
<p>Are the design documents baselined?</p>		
<p>Are the requirements baselined?</p>		
<p>Have Test procedures been written and approved? Are they of sufficient detail? Do they exist for Unit test? Do they exist for CSCI level testing Do they exist for CSCI integration level testing? Do they exist for Software System level testing? Will these tests be used for acceptance testing to the system? Are these procedures in SCM? Are they baselined?</p>		
<p>Do some software requirements need to be tested at the systems level or complete verification? Are these documented? Does the systems level test procedures adequately cover these? Does the Requirements/verification matrix indicate which requirements are tested at the systems level?</p>		
<p>For System level testing,: Has software been officially accepted by systems? (sign-off, baselined) Are software testing facilities maintained for any regression testing?</p>		
<p>Unit testing procedures and results maintained via SCM?</p>		
<p>Is there auto generated code?</p>		
<p>Is unit testing planned for auto generated code? Are there procedures for testing unit level auto generated code?</p>		
<p>Implementation personnel familiar with development environment? Language? and tools? Sufficient trained coders (e.g. understand OOA, OOD, C++, Formal Methods, etc., whatever is needed)? Sufficient expertise in (not first or second time ever done, not just trained) ?</p>		
<p>Coders are sufficiently familiar with project function/design needs? Or coders have ready access to someone who does - someone with sufficient expertise and whose time is available for participation in code walk-throughs/inspections and for technical questions?</p>		
<p>Is there sufficient equipment?</p>		
<p>Are there build procedures? Are they documented? Are they in SCM? Are they being followed?</p>		

<p>Are there burn procedures for any PROMS? ROMS? EEPROMS? Are they documented? Are they in SCM? Are they being followed?</p> <p>Do they include method for clearing PROMs (if applicable) and checking them for defects prior to burning? Does procedure have method to determine and record the checksum(s)?</p>		
<p>Are test plans complete? Are they still being worked? Do they include Unit level testing? CSCI level testing? Integration testing CSCIs? System level testing?</p>		
<p>Is the test/requirements matrix up to date?</p>		
<p>Integration and Systems Testing</p>		
<p>Are review activities and schedules well defined and coordinated?</p>		
<p>Sufficient experienced Test personnel? Experienced on similar projects? Experienced with this project? Experienced with test equipment, set-up, simulators, hardware? Experienced with development environment?</p>		
<p>Is the Software Test Plan being followed? Does it need to be modified? Does it include COTS? Does it include auto generated code?</p>		
<p>Are there well written, comprehensive test procedures? Are they up to date? Do they indicate the pass/fail criteria? Do they indicate level of regression testing?</p>		
<p>Test reports are written at the time of the tests?</p>		
<p>Test reports are witnessed and signed off by SPA?</p>		
<p>Is the test/requirements matrix up to date?</p>		
<p>Is there a known recourse/procedure for testing procedure changes? Is it understood? Is it used? Does it take into account changes to parent documents? Does it take into account subsequent changes to child documents? Does it take into account regression testing?</p>		
<p>Is there a known recourse/procedure for requirements changes? Is it understood? Is it used? Is it adequate, does it need to be altered? Does it take into account changes to parent documents? Does it take into account subsequent changes to child documents?</p>		
<p>Is there Software Configuration Management (SCM) (for tracking baselined changes and progress) Is it being used? Are backups performed automatically on a regular basis?</p>		
<p>Is there formal SCM and Baselining of Requirements and Design?</p>		
<p>Are the design documents formally baselined and in SCM?</p>		
<p>Are the software requirements formally baselined?</p>		

<p>Have Test procedures been written and approved? Are they of sufficient detail? Do they exist for Unit test? Do they exist for CSCI level testing Do they exist for CSCI integration level testing? Do they exist for Software System level testing? Will these tests be used for acceptance testing to the system? Are these procedures in SCM? Are they baselined?</p>		
<p>Do some software requirements need to be tested at the systems level for complete verification? Are these requirements verification procedures documented? Where? In Software test Procedures? In Systems Test Procedures? Do the systems level test procedures adequately cover these? Does the Requirements/verification matrix indicate which requirements are tested at the systems level?</p>		
<p>For System level testing,: Has software been officially accepted by systems? (sign-off, baselined) Are software testing facilities maintained for any regression testing?</p>		
<p>Is Firmware ready and tested? Is it Baselined and in SCM?</p>		
<p>Is there Flight and/or engineering model Hardware to test on? If engineering model, are differences to flight h/w known, recorded and can be accounted for verification of software? Is engineering model stable? Is Flight hardware stable? If not, is there a log kept of changes to the hardware which is public and easily accessible? Are the impacts to software and software testing reported? Discussed? Known?</p>		
<p>Is there separate test personnel that have not been designer or coders for this task? Do they need training? Is time allowed for their unfamiliarity with the system?</p>		
<p>On the flip side, are testers too familiar with software? Will they have a tendency to brush over problems or fix problems without going through proper channels/procedures?</p>		
<p>Have requirements/design/code personnel been moved to other tasks and are no longer available to support testing or error correction?</p>		
<p>Are test pass/fail criteria known and understood?</p>		
<p>Is regression testing planned for? Is there time in the schedule for it? Have estimates been made at each test point of the amount of regression testing necessary to cover fixes if test fails? (e.g. certain failures require complete end-to-end retesting, others may require only retesting of that test point.)</p>		
<p>Is ground software (or other related software) available for testing or for use in testing flight s/w</p>		
<p>Has testing of COTS at the software system level been adequately covered and documented? Are there test procedures specifically for proving integration of COTS? Does the Requirements to Test Matrix indicate where COTS are</p>		

involved?		
Has testing of COTS at the system level been adequately covered and documented?		
<p>Is there good configuration management in place?</p> <p>Is it used?</p> <p>Is there version control?</p> <p>Error/failure tracking in place?</p> <p>PRACA and/or S/W Change Records created?</p> <p>Tracked to closure?</p> <p>Error correction written into each new release of a module (in code comments, in file header, in SCM version description)</p> <p>Are incorporated PRACAs listed in build release version descriptions?</p>		
<p>Will a tight schedule cause:</p> <p>Dropping some tests?</p> <p>Incomplete regression testing?</p> <p>Dropping some fixes?</p> <p>In sufficient time to address major (or minor) design and/or Requirements changes?</p> <p>No end-to-end testing?</p> <p>How are these issues to be addressed?</p> <p>Who makes these decisions? The Change Control Board?</p> <p>How are they recorded?</p> <p>Does the Version Description Document (VDD) indicate true state of delivered software?</p>		
Has all the slack/contingency time on the critical path been used up?		
Are software metrics kept and reported regularly? Monthly?		
<p>Are deviations to the development plan being tracked? Trended?</p> <p>Are the trends reported in a manner to allow timely and appropriate software and project management decisions?</p>		

Acceptance Testing and Release	<u>RISK</u>	<u>ACTION</u>
Has pre-ship review already taken place?		
Actual Flight Equipment available for software testing? Logbook and test procedure record actual flight hardware used for testing?		
Pass/Fail Criteria established and followed?		
Regression testing procedure documented and known? Is it used?		
Procedure to handle PRACAs at acceptance level documented? Change review board in place? Configuration management of changes? PRACA/SPCR log maintained with status?		
Systems level testing adequate to insure software requirements or some software level testing done separately and documented?		
Appropriate personnel to witness and sign-off and testing? SPA or QA involved?		
Are all parts of the architecture verified on the ground prior to flight?		
A complete VDD exists? All delivered software release versions listed? All COTS and their versions listed? All hardware versions appropriate for this release noted? SCM release description (s) Build procedures? Burn procedures? Installation procedures? List of all incorporated (closed) Problem Reports and Change Requests? List of all outstanding Problem Reports and Change Requests? List of any known bugs and the work-arounds? List changes since last formal release? List of all documentation that applies to this release? If known discrepancies to hardware, documentation, etc. are these listed and discussed?		
Clean customer handoff: Up to date documentation? User/Operations Manual? Code Configuration Managed? All PRACAs & SPCRs closed?		
Good configuration management wrap-up: Is there a method for future updates/changes in place? Proper off-site storage of data, software and documentation? What happens to SCM and data when project is over?		
Additional Risks:	<u>RISK</u>	<u>Action:</u>
