SeniorConnect Project
Risk Management Plan

Version 2.0

30/09/2015

GruFamily Project Team
Nanyang Technological University
50 Nanyang Avenue Singapore
639798

Table of Contents

Revision History

Revision	Author	Date	Comments
1.0	Ma Xiaoxue Li Yishan	27/09/2015	Initial version
1.1	Ma Xiaoxue	29/09/2015	First revision, merged content. Ensured consistency and removed duplicated content.
2.0	Ma Xiaoxue Li Yishan	30/09/2015	Final version
2.1	Wong Way-ne	03/11/2015	Corrections, added additional stategies

SeniorConnect Project
Risk Management Plan

Version 2.0

30/09/2015

Risk Management Plan Approvals:

LI YISHAN — 30/09/2015

SQA Manager **Date**

刘曙晴 — 30/09/2015

Project Manager **Date**

1. Introduction

1.1. Purpose and Scope

The purpose of this Risk Management Plan (RM Plan) is to document the standards and procedures that should be followed by SeniorConnect (SC) project for identifying risks and drawing up plans to minimize their impacts on the project. This plan for risk management is only one sub-plan for the entire SC project's planning documentation. In this document context, risk is defined as the possibility of suffering a negative impact to the project, product or business. For example, typical risks can be identified with the project would be scarce resources, delay in schedule and overrun of budget.

The scope of this plan covers all RM processes within GruFamily project team. The standards and procedures defined by this RM plan should be followed by all sub-teams for carrying out RM activities. This plan shall also keep a log of the identified risks for SC project. The log shall serve the purposes of risk identification, documentation, analysis, response planning and monitoring. At this stage, response strategies are only planned for risks assessed to be of high or intermediate priority. Documentation of any RM activities carried out after the establishment of this plan shall follow the standards in the plan. Those before the establishment of this plan shall be revised in accordance to the plan.

1.2. Definition and Standard

SC project should conform to IEEE Standards for Software Engineering in the process of identifying, analyzing, responding and monitoring the risks. The GruFamily project team should conduct risk management to systematically control the uncertainty in the project's ability to meet cost, schedule, and performance objectives.

1.2.1. IEEE Standards for Software Engineering

Risk management is part of the overall management process related to potential technical, cost and schedule risks. Risk management is a tool for problem prevention: identifying the things that could go wrong, assessing their impact, and determining which potential problems need to be avoided. Risk management is an activity that should be performed by all levels of the project to ensure adequate coverage of all potential problem areas. Open communication is required to provide all project personnel with the freedom to identify issues without negative consequences to themselves. Joint management of risks between acquirer and supplier, with support from developer/maintainer/operator, is necessary to enable identification of the most important risks to the program and to support efficient allocation of mitigation resources. Risk management may make use of other supporting processes, such as problem resolution, quality assurance, and joint reviews.

1.3. Risk Management Approach

The overall risk management approach follows the standard risk management model developed by Software Engineering Institute (SEI) as show in the following figure.

Figure 1.1 - Risk Management Model

1.3.1. Risk Identification

During risk identification, the potential project, product and business risks, and risk types are identified – refer to Section 3 for details.

1.3.2. Risk Analysis

During risk analysis, the probability of the risk occurring and seriousness of identified risks effects are assessed – refer to Section 4 for details.

1.3.3. Response Planning

During response planning, risk management including contingency plans are developed – refer to Section 5 for details.

1.3.4. Risk Monitoring

During risk monitoring, identified risks are under surveillance; if applicable, corrective action plans are developed, implemented, and monitored – see section 6 for details.

1.4. Risk Management Process

Risk Management	
Input	- Risk Management Plan Template - Project Plan - Other software documentations, e.g. SRS - Risk categorization model - Risk probability and effect assessment models - Team level standards, practices, guidelines as tailored to this project
Entry Criteria	- Project Manager has directed enough attention to RM processes - Personnel have been assigned for RM activities - All inputs listed are available
Procedures & Measurements	- Risk identification - Risk Analysis - Response planning - Risk monitoring
Exit Criteria	- Review and approval of the RM plan - Review of the Risk Log - Completion of the risk prioritization - Successful development of response planning strategies for each of the identified risk
Output	- Risk Management Plan - Risk Log

2. Roles and Responsibilities

The following responsibility matrix shows the Risk Management responsibility for each role in the GruFamilly project team for SC project.

	Project Manager	QA Manager	QA Engineer	Lead Developer	Front-end/ Back-end Developer	Release Engineer /Manager
Overall responsibility of managing the risks	×					
Review Risk Management plan	×	×	×	×	×	×
Approve Risk Management plan	×	×				×
Analyze taxonomy of potential risks area to identify a candidate list of risks			×		×	
Document identified risks in the Risk Log			×		×	
Analyze probability of occurrence and severity of the risks			×		×	
Prioritize risks according to calculated risk levels			×			
Review Risk Log	×	×	×	×	×	×
Develop risk avoidance, minimization and contingency plans	×	×	×	×	×	×
Coordinate the implementation of avoidance, minimization and contingency plans	×	×				×
Implement	×	×	×	×	×	×

avoidance, minimization and contingency plans						
Track and control risk management process	×	×	×			
Ensure the risk management processes are carried out in accordance to standards and procedures defined in RM plan		×	×			

3. Risk Identification

3.1. Background

During risk identification, the potential project, product and business risks and risk types should be identified. With the help of the risk categorization model, the risk identification process is ensured to be carried out in a systematic and exhaustive way. The coverage of the identified risks is ensured. The identified risks shall be documented in the Risk Log by specifying the description and estimated impact/symptoms of the risk. RM is an iterative process. New risks can be identified continuously during the entire project. The risk categorization followed by SeniorConnect project is shown in Figure 3.1.

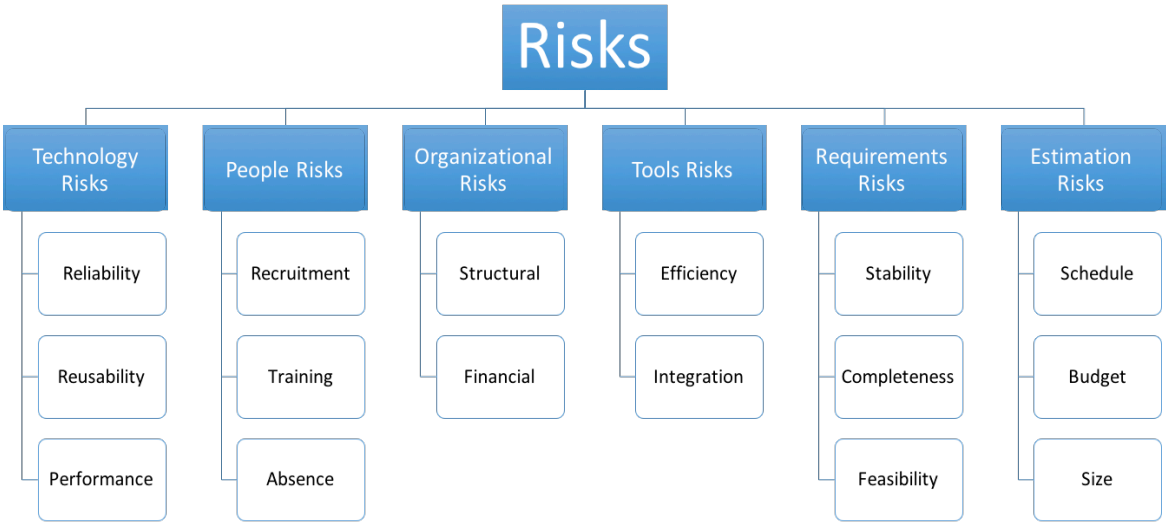

Figure 3.1– Risk Categorization Model

3.2. Sources

Risk identification is done throughout the development life-cycle of a project. However, it is advisable to identify a majority of the risks in the early stage so corresponding response planning and monitoring can be prepared and implemented in advance. The following tools and techniques should be considered for risk identification:

- Analysis of high-level deliverables
- Analysis of the WBS, project assumptions and project schedule
- Analysis of scope against requirements

- Input from project team, stakeholders and sponsors
- Experience from previous projects and lessons
- SQA audits and reviews
- Performance and status reports

3.3. Documentation

All identified risks should be documented and entered into the Risk Log, which can be found in Appendix of this document. During risk identification, the following information should be identified and documented.

- Risk category
- Risk indicator and/or description
- Potential effect
- Identified By
- Date Raised

4. Risk Analysis

4.1. Background

After the potential risks have been identified and documented in the Risk Log, risk analysis should be performed. During risk analysis, each potential risk should be analyzed for:

- The probability that the risk will occur
- The effects of the risk if it occurs

Risk probabilities are defined in Section 4.2. Risk effects are defined in Section 4.3. The risk probability and effect matrix is shown in section 4.4. The matrix shows the combination of effect seriousness and probability that in turn yield a risk priority (shown by the red, yellow, and green colored shadings).

Risk priority is utilized during response planning and risk monitoring (see Sections 5 and 6). It is critical to understand the priority for each risk as it allows the project team to properly understand the relative importance of each risk.

4.1.1. Analysis Technique

Risk analysis can be qualitative or quantitative. Qualitative analysis is a quicker and usually more cost-effective way to analysis risks (as opposed to quantitative analysis). Quantitative analysis utilizes techniques such as simulation and decision tree for risk analysis. In SeniorConnect project, qualitative analysis should be conducted together with quantitative analysis with the goal of gathering data on:

- The likelihood of the risk occurring (using table from Section 4.2)
- The qualitative impact on the project (using table from Section 4.3)
- The priority of the identified risk (using table from Section 4.4)

4.2. Risk Probability

According to the probability of occurrence, risks can be classified into three probability categories. The probability range and description of each category is shown in Table 1. During risk analysis, the potential likelihood that a given risk will occur should be assessed, and an appropriate probability category should be selected for the risk from the following table.

Probability Category	Probability	Description
High	0.70	Risk event more likely than not to occur
Moderate	0.50	Risk event may or may not occur
Low	0.30	Risk event less likely than not to occur

Table 1 – Risk Probability Categories

4.3. Risk Effect Seriousness

According to the seriousness of effect, risks can be classified into three severity scales. The seriousness of effects can be assessed against multiple project areas, namely project cost, schedule, scope, and/or quality. In the event when more than one criterion is affected by the risk and the scales are different, the higher seriousness score should be utilized. The scales of risk effect seriousness are shown in Table 2. During risk analysis, the potential effect of each risk is analyzed, and an appropriate seriousness level (0.20. 0.50, or 0.80) is selected from the table below.

Project Objective	Low 0.20	Tolerable 0.50	High 0.80
Cost	Insignificant cost impact	15-40% cost impact	>40% cost impact
Schedule	Insignificant schedule impact	5-20% schedule impact	>20% schedule impact
Scope	Minor areas impacted	Major areas impacted	Product becomes effectively useless
Quality	Only very demanding applications impacted	Some sacrifices in major functionalities	Product becomes effectively useless

Table 2 –Risk Effect Seriousness Scales

4.4. Risk Probability and Effect Seriousness Matrix

Once the appropriate risk probability and effect seriousness are selected, the risk priority can be determined. The risk probability and effect seriousness matrix is shown in Table 3. The cells in the same row are of same probability of occurrence; and cells in the same column are of same identified effect seriousness. The matrix shows the combination of risk effect seriousness and probability, and is utilized to decide the relative priority of risks. Risks that fall into the red-shaded cells of the matrix are the highest priority, and should receive the majority of risk management resources during response planning and risk monitoring. Risks that fall into the yellow-shaded cells of the matrix are the next highest priority, followed by risks that fall into the green-shaded cells.

Probability	Threats		
0.70	0.14	0.35	0.56
0.50	0.10	0.25	0.40
0.30	0.06	0.15	0.24
	0.20	0.50	0.8

Table 3 – Risk Probability and Effect Seriousness Matrix

4.5. Documentation

The results of risk analysis should be documented in the Risk Log. The following information shall be entered in the document after risk analysis.

- Risk probability
- Risk effect seriousness
- Risk priority with matrix score – computed by the Risk Log spreadsheet in Appendix after probability and severity are entered

5. Response Planning

5.1. Background

The target of response planning is to achieve a better risk management for each identified risk or for each risk of high-priority on the Risk Log at least. During response planning, strategies and/or plans should be developed to minimize the effects of the risk to the extent that the risk can be controlled and managed. Higher priority risks should receive more attention during response planning than lower priority risks. There are several methods for responding to risks, namely avoidance strategy, minimization strategy and contingency plan. The risk strategies and/or plans should be discussed and analyzed against every important risk during project team internal meeting. In this way, a suitable risk response plan can be developed for SC project. Each of the strategy will be discussed in greater details in following section, e.g. section 5.2.

5.2. Risk Strategies

5.2.1. Avoidance Strategies

Avoidance strategies help reduce the probability that the risk will arise. Some risks can possibly be avoided by applying an alternative approach with controllable risk. Risks that are identified early in the project can be avoided by clarifying requirements, obtaining more information, preparing back-ups, reallocating resources or obtaining expertise.

Risk avoidance strategies involve changing aspects of the overall project management plan to eliminate the threat, isolating project objectives from the risk's impact, or relaxing the objectives that are in threatened (e.g. extending the schedule or reducing the scope). It may not completely eliminate the risk, but only reduce the risk to a certain level that can be managed.

5.2.2. Minimization Strategies

When risk cannot be avoided, the effect of loss can often be minimized in terms of frequency and severity. Risk minimization strategies involve reducing the adverse impact of project and/or product risks to an acceptable level. Compared to avoidance strategies, minimization strategies do not change the original approach to project management, but alter the effects of original approach instead. Taking early and pro-active action against a risk is often more effective than attempting to repair the damage a realized risk has caused.

5.2.3. Contingency Plan

Contingency plans are solutions that are prepared beforehand. When the risk arises, the contingency plans should be applied immediately and effectively. Contingency plan aims to reduce the severity of existing risks to an acceptance level. Compared to risk avoidance, contingency plan is more passive and should focus on handling and containing adverse impacts of top-priority risks.

5.3. Documentation

The results of response planning should be documented in the Risk Log spreadsheet in Appendix. The following information shall be entered in the document.

- Response strategy (avoidance strategy, minimization strategy and/or contingency plan) with detailed description

6. Risk Monitoring

6.1. Background

Risk monitoring is a final step that makes the risk management a closed-loop process. The process of risk management is iterative as newly unidentified risks may occur at any stages of the project. After identification, the newly detected risk should follow the risk management cycle and go through all stages.

Risk monitoring ensures most risks are foreseen and under surveillance by the project team. Identified risks are tracked on a regular basis in terms of occurring probabilities and resulting severity. Risk indicators are effective tools used to detect the risk on an early stage. Each key risk, e.g. risks on the top-level risk-identification checklist, should be discussed at management progress meetings.

The risk monitoring process should be reviewed by SC project team and audited by SC SQA team to make sure that all the planned activities have been carried out in accordance to this RM plan. Project Manager should organize regular Management Process Review to monitor the project progress, check statuses of identified risks and actively identify new risks.

During risk monitoring, the following tasks are performed:

- Review the Risk Management Plan
- Review the Risk Log
- Review and audit risk management process
- Review project progress and status
- Keep track of identified risks and monitor risk indicators
- Identify, analyze, and plan for new risks
- Re-analyze existing risk risks to see if the probability, impact, or priority has changed and adjust response strategy if necessary
- Review the execution of risk responses and analyze their effectiveness

6.2. Documentation

The results of risk monitoring should be documented.

- Status of identified risks should be documented in the Risk Log:
    - Supervised – Risk has been identified and analyzed and is under supervision from SC project team.
    - Triggered – Risk indicators has shown noteworthy alerts. Risk has been realized and response strategies should be executed.
    - Resolved – Realized risk has been contained.

  - Retired – Identified risk no longer requires active monitoring (e.g. risk trigger has passed)

- RM Plan and Risk Log review results – Review Form Template (SQAP Appendix II-B)
- Management Process Audit result – Management Review Form (SQAP Appendix II-H)
- RM Processes audit results – Process Audit Form (SQAP Appendix III-E)

Appendix - Risk Log

Risk Category	Risk Description	Probability of Occurrence	Seriousness of Effects	Priority	Rank	Strategies	Status
Organizational	The organization is restructured so that different management personals are responsible for the project.	High	High	High	1	Prepare briefing presentation and detailed document for management showing how the project is progressing and making a very important contribution to the goals of the business. Keep effective and frequent communication with the new management team.	
People	It is impossible to recruit staff with the skills required for the project.	High	High	High	1	Alert customer timely of potential difficulties and the possibility of delays; investigate buying-in components efficiently.	
Estimation	Team may underestimate the cost beforehand and thus do not have enough budget during the development.	Moderate	High	High	2	The team should have a detailed budget. Instead of having a general one, the budget should be broken down into small components and each component should be analyzed and forecasted with reasonable cost.	
People	Experienced staff may leave the project before it is finished.	Moderate	High	High	2	Reorganize team so that there is more overlap of work and people therefore understand each other's jobs.	
People	Key staff fall ill at critical times in the project.	Moderate	High	High	2	Reorganize team so that there is more overlap of work and people therefore understand each other's jobs. If the situation is urgent, invite experienced staff from other teams to contribute.	
Requirements	Changes to requirements that require major design rework are proposed.	Moderate	High	High	2	Derive traceability information to assess requirements change impact, maximize information hiding in the design.	
Technology	Software components that should be reused contain defects which limit their functionality.	Moderate	High	High	2	Replace potentially defective components with bought-in components of known reliability.	
Technology	The database used in the system cannot process as many information per second as expected.	Moderate	High	High	2	Investigate the possibility of buying a higher- performance database.	

Estimation	The time required to develop the software is underestimated.	High	Tolerable	High	3	More research and analysis should be taken before the start of development. All team members should have discussion together about the schedule, to make sure appropriate plan have been made. Investigate buying components, investigate use of a program generator.	
Estimation	The size of the software is underestimated.	High	Tolerable	High	3	More research and analysis should be taken before the start of development. All team members should have discussion together about the software complexity to make sure appropriate estimation about the software size have been made. Investigate buying in components, investigate use of a program generator.	
Requirements	Gap between Requirements And Developed Functionality It is possible that the functions developed by the team cannot match the requirements elicited beforehand.	High	Tolerable	High	3	Requirements should be realistic and appropriate. Thus more analysis and discussion should be taken beforehand. Requirement documents should be reviewed regularly during the development to ensure that crucial requirements are matched.	
Tools	WebRTC (Real-time Communication) tools cannot be integrated.	High	Tolerable	High	3	More research and analysis should be taken before the start of development. Experienced developers should examine the integration ability of WebRTC. If the result is not favorable, use alternative tools.	
Estimation	The rate of defect repair is underestimated.	Moderate	Tolerable	Intermediate	4	Replace potentially defective components with bought- in components of known reliability.	
People	Human Error Team members may make some mistakes accidently during the whole process of the project. These mistakes may cause data inconsistency, system errors and project delay.	Moderate	Tolerable	Intermediate	4	In order to avoid mistakes, every team member should do a review for the work done. Peer review should also be adopted, especially for crucial part of the project.	

Requirements	Customers fail to understand the impact of requirements changes.	Moderate	Tolerable	Intermediate	4	Emphasis the meaning of requirements changes by onsite demo, onsite trial and other methods that let customers have a real experience using the product.	
Technology	The underlying technology on which the system is built is superseded by new technology.	Moderate	Tolerable	Intermediate	4	Before the project starts, technology used should be examined with extensibility and future trends. If new technology or versions supersedes the used technology, examine the probability for replacing using a cost-benefit analysis.	
Tools	Real-time Communication tools which support the project do not perform as anticipated	Moderate	Tolerable	Intermediate	4	More research and analysis should be taken before the start of development. Experienced developers should examine the functionalities of WebRTC. If the result is not favorable, use alternative tools.	
Estimation	Specifications of essential interfaces are not available on schedule.	Low	High	Intermediate	5	Investigate the reasons that cause the delay. Send more experienced staff to speed up the interface specification process.	
Organizational	Organizational financial problems force reductions in the project budget.	Low	High	Intermediate	5	Prepare briefing presentation and detailed document for management showing how the project is progressing and making a very important contribution to the goals of the business.	
Tools	Hardware that is essential for the project will not be delivered on schedule.	Low	High	Intermediate	5	Keep in contact with suppliers about delivery details and show great emphasis on the timely delivery. If the hardware is not delivered online, reschedule the hardware-relevant procedures to minimize the impact.	
Organizational	There will be a change of organizational management with different priorities.	Low	Tolerable	Low	6	Prepare briefing presentation and detailed document for management showing how the project is progressing and making a very important contribution to the goals of the business.	
People	Required training for staff is not available.	Low	Tolerable	Low	6	Currently unavailable due to low priority	
Tools	The data generated by Real-time Communication tools is inefficient.	Moderate	Low	Low	7	More research and analysis should be taken before the start of development. Experienced developers should examine the functionalities of WebRTC. If the result is not favorable, use	

						alternative tools.	

Reference

Boehm, Barry W., “Software Risk Management: Principles and Practices,” IEEE Software, January 1991.

CZ3002 notes from Nanyang Technological University

Risk Management Plan Template