QUANTIFYING RISK MANAGEMENT PROCESS IN A SOFTWARE ORGANIZATION

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

CENKLER YAKIN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
INDUSTRIAL ENGINEERING

APRIL 2006

Approval of the Graduate School of Natural and Applied Sciences.

_____

Prof. Dr. Canan ÖZGEN
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Prof. Dr. Çağlar GÜVEN
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Prof. Dr. Ömer SAATÇİOĞLU
Supervisor

Examining Committee Members

Prof. Dr. Halim DOĞRUSÖZ (METU, IE) _____

Prof. Dr. Ömer SAATÇİOĞLU (METU, IE) _____

Asst. Prof. Dr. Sedef MERAL (METU, IE) _____

Asst. Prof. Dr. Engin KÜÇÜKKAYA (METU, BA) _____

M.Sc. Serkan ÇAK (STM A.Ş.) _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Cenkler YAKIN

Signature :

ABSTRACT

QUANTIFYING RISK MANAGEMENT PROCESS IN A SOFTWARE ORGANIZATION

Yakın, Cenkler

M.S., Department of Industrial Engineering

Supervisor: Prof. Dr. Ömer SAATÇİOĞLU

April 2006, 200 pages

This study presents a quantifying risk management process and its application on a software organization in terms of risk items mitigated, exposures covered, costs, and expected exposures covered.

Risk management is defined as setting forth a discipline and environment of proactive decisions and actions to assess continuously what can go wrong (risks), to determine what risks are important to deal with, and to implement strategies to deal with those risks. Risk management can be applied in all of the business areas. In the literature, there are sources for risk management. Some of them are qualitative, and some of them are quantitative. However, there is no much source about the application study of a quantifying risk management process on a software organization.

In order to obtain insight about this issue, this study presents a quantifying risk management system to the literature and also compares the quantifying risk management policies on the data set of a software organization by finding out and analyzing their performance with respect to designated decision parameters and preference profiles for risk items mitigated, exposures covered, costs, and expected exposures covered. At the end of this study, suitable quantifying risk management

policies for each profile are recommended by considering the analysis of the data set as base.

Key Words: Quantifying risk management, software risk management, risk prioritization method, risk threshold

ÖZ

SAYISALLAŞTIRILMIŞ RİSK YÖNETİMİ SÜRECİNİN BİR YAZILIM ŞİRKETİNE UYGULANMASI

Yakın, Cenkler

Yüksek Lisans, Endüstri Mühendisliği Bölümü

Tez Yöneticisi: Prof. Dr. Ömer SAATÇİOĞLU

Nisan 2006, 200 sayfa

Bu çalışma, sayısallaştırılmış bir risk yönetimi süreci sunulmasını ve bu sürecin bir yazılım şirketi için önlenen risk maddeleri, kapsanan risk değerleri, maliyetler ve kapsanan ortalama risk değerleri açısından uygulamalarını değerlendirmektir.

Risk yönetimi; riskleri belirleyebilmek, hangi risklerin önemli olduğuna karar verebilmek ve bu risklerle uğraşmak için stratejilerin uygulanmasını sağlamak için proaktif karar ve faaliyetlerin alınmasını sağlayacak disiplinin ve ortamın kurulmasını tanımlamaktır. Risk yönetimi, tüm iş sektörlerinde kullanılabilir. Literatürde risk yönetimi için kaynaklar vardır. Bazıları sözel, bazılarıysa sayısal risk yönetimi içindir. Fakat, literatürde sayısallaştırılmış bir risk yönetimi sürecinin bir yazılım şirketinde uygulanma çalışması hakkında fazla kaynak yoktur.

Bu husus hakkında bilgi sağlayabilmek için, bu çalışma literatüre sayısallaştırılmış bir risk yönetimi sistemi sunar, ve sayısallaştırılmış risk yönetimi politikalarını bir yazılım şirketinin verilerini baz alarak önlenen risk maddeleri, kapsanan risk değerleri, maliyetler ve kapsanan ortalama risk değerleri açısından belirlenen karar parametrelerine ve profillere göre analiz ederek kıyaslar. Bu çalışmanın sonunda, veri kümesinin analizlerine göre her bir profil için uygun sayısallaştırılmış risk yönetimi politikaları önerilir.

Anahtar Kelimeler: Sayısallaştırılmış risk yönetimi, yazılım risk yönetimi, risk önceliklendirme metodu, risk eşik değeri

To My Parents

ACKNOWLEDGEMENTS

The author wishes to express his deepest gratitude to his supervisor Prof. Dr. Ömer Saatçioğlu for his guidance, advice, criticism, encouragements and insight throughout the research.

TABLE OF CONTENTS

APPENDICES

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

CHAPTER 1

INTRODUCTION

In each business area, there is a possibility of risk occurrence about any subject. Risk is a possible future event with a negative impact, so may cause the business to deviate from its targets. In order to prevent the deviation, risk management techniques are applied. Risk management aims to identify potential problems before they occur, so that risk-handling activities are planned as needed to mitigate adverse impacts on achieving objectives. The term risk management is applied in a number of diverse disciplines. People in the fields of statistics, economics, psychology, social sciences, biology, engineering, toxicology, systems analysis, operations research, and decision theory, etc have been addressing the field of risk management.

Risk management can be performed either qualitatively or quantitatively. Qualitative risk management depends on the subjective ideas of the people. A potential risk item can be evaluated as risk by some people in the organization, but can be concluded as non-risk item by the other ones in the organization. However, quantitative risk management is more objective that, potential risk items are evaluated by means of quantitative values of the parameters. Finally it is concluded that whether it is risk or not according to the quantitative results, not based on people' subjective ideas.

In this study; quantifying risk management methods are built, and these methods are applied on a software organization since the organization need to have quantifying risk management process and see its applications (the name of the software organization is not mentioned because of the security reasons). In this study, quantifying risk management policies are defined. These policies are based on quantifying risk management methods. Besides these, different preference profiles are defined according to the defined aims and expectations of the software

organizations. Quantifying risk management policies are evaluated with respect to the outcomes for each preference profile. These policies are ranked for each preference profile. During the usage of the study, the organization determines its profile, and chooses the best policy from ranked policies for the related profile. Finally, organization applies the choosen policy in its risk management process.

This study is presented as follows. In Chapter 2; risk concept, risk management, the issues regarding principles of risk management, functions of risk management, and software risk management are described in detail. Chapter 3 initially puts forward the information about the risk management and quantifying risk management in the literature, and the aims of the study. Then, the parameters to build the quantifying risk management methods are defined, and the values for these parameters are calculated in the tables from the data set of the software organization. These parameters are given in the titles of 'Risk Analysis' and 'Risk Control'. Chapter 3 continues by defining the thresholds which are used to choose 'mitigate' or 'monitor' decisions in the study. The succeeding chapter, namely Chapter 4, provides the definitions and contents of the quantifying risk management policies and preference profiles. Then, application of the policies is performed to the data set of the organization formed in Chapter 3. Results of application of policies are presented in Chapter 4. This chapter also evaluates the policies, and analyzes the results to rank the policies for each preference profile in terms of decision parameters defined in Chapter 3. Finally, in Chapter 5, the study is concluded by summarizing the study, and describing the potential research opportunities that may be considered in the future.

CHAPTER 2

BACKGROUND AND LITERATURE SURVEY

2.1. Risk Concept

There are a number of definitions and uses for the term risk, but no universally accepted definition. What all definitions have in common is agreement that risk has two characteristics

- **uncertainty** - an event may or may not happen
- **loss** - an event has unwanted consequences or losses

According to Lowrance, risk is the measure of the probability and severity of adverse effects [19]. Fairley has the similar definition of risk as "the probability of incurring a loss or enduring a negative impact" [9]

Webster's dictionary defines risk as the possibility of suffering loss, injury, disadvantage, or destruction [3]. SEI (Software Engineering Institute) uses the Webster's definition of risk "the possibility of suffering loss". In a development program, the loss could be in the form of diminished quality of the end product, increased costs, delayed completion, or failure.

Risk can be defined in terms of project side. A project risk is defined as "an uncertain event or condition that, if it occurs, has a negative effect on a procet's objectives" according to Carbone and Tippett [4]. Ward and Chapman define risk as uncertain event or set of circumstances that, should it occur, will have an effect on the achievement of the project's objectives [28].

In business terms, Blakley and McDermott see risk as the possibility of an event which would reduce the value of business were it to occur [2]. Dedolph states that

"risk can be defined as the possibility of harm or loss in the business. Typically, risks are described as some kind of event that may or may not occur, coupled with a consequence that follows if the event occurs. This definition leads naturally to considering the probability of the risk event and the cost(s) associated with the consequence" [6].

Risk is undesirable event. In some situations, risk is equated to a possible negative event. Levin and Schneider define risk as "… events that, if they occur, represent a material threat to an entity's fortune" [18]. Using this definition, risks are the multiple undesirable events that may occur according to Aubert, Patry, and Rivard [1].

Since risk identifications performed on the projects of the organization, Carbone and Tippett's definition for risk [4] is the most suitable in this study.

Keefer's definition for relative position of "risk" against "opportunity", "problem" and "success" is given in Table 1. [13]

Table 1 Risk Concept

	Present	***Future***
Negative	**Problem:** Present event with a negative impact	**Risk:** Possible future event with a negative impact
Positive	**Success:** Present event with a positive impact	**Opportunity:** Possible future event with a positive impact

An Example of Risk

Higuera and Dorofee give an example of risk: "Company X has just introduced object-oriented technology into its organization. They see this new technology as having considerable competitive advantage in the future because of its potential for asset reuse in their major product lines. Although many people within the

organization are familiar with the technology, it has not been part of their development process, and their people have very little experience and training in the technology's application." [12]

Here, the risk is: Given the lack of experience and training, there is a possibility that asset reuse will not be realized before losing market share.

Non-Example of Risk

Higuera and Dorofee give a nonexample of risk: "Company Y is developing a flight control system. During system integration testing the flight control system becomes unstable because processing of the control function is not quick enough during a specific maneuver sequence." [12]

This is not a risk since the event is a certainty – it is a problem

2.2. Risk Management

Doherty states that risk should be handled by reducing the probability or magnitude of loss, and by avoiding the activity that gives rise to loss [7]. Knowing that risks actually exist and must be carefully considered is a discipline called risk management according to Maude and Willis [21]. Schmit, and Roth describe risk management as the performance of activities designed to minimize the negative impact (cost) of uncertainty (probability) regarding possible losses [26]. According to Kloman, risk management is a discipline for living with the possibility that future events may cause adverse effects [16]. Ward highlights the project risk management's defintion as a subset of project management with four component processes: risk identification, risk quantification, risk response development, and risk response control [30]. Higuera, and Dorofee define risk management as setting forth a discipline and environment of proactive decisions and actions to [12]

1. assess continuously what can go wrong (risks).

2. determine what risks are important to deal with.

3. implement strategies to deal with those risks.

“Today, effectively managing risk is an essential element of successful project management. Proper risk management can assist the project manager to mitigate against both known and unanticipated risks on projects of all kinds. Failure to perform effective risk management can cause projects to exceed budget, fall behind schedule, miss critical performance targets, or exhibit any combination these troubles” mentioned by Carbone, and Tippett [4]. Even Elkington, and Smallman claim that “the less predictable nature of projects makes them riskier than day to day business activities. Hence, risk management is an integral part of project management and most large companies put substantial resources into the management of business risk” [8].

SEI (Softare Engineering Institute) explains the purpose of risk management as to identify potential problems before they occur, so that risk-handling activities may be planned and invoked as needed across the life of the product or project to mitigate adverse impacts on achieving objectives [27].

Boehm evaluates the objective of risk management as to identify, analyze, prioritize, resolve and monitor all risks to avoid adverse impact on project goals [3]. According to Dedolph, risk management activities have three primary goals: identifying, analyzing and mitigating risks [6].

Hamdi, and Boudriga categorize risk management approaches into two groups: qualitative risk management and quantitative risk management. The former consists in prioritizing the various risk elements in subjective terms. The latter is based on quantifying the magnitude of risk created by the exposure of the target system to negative events. Techniques belonging to the first class are more used than the others as they are more easy to implement [11]. Quantitative techniques which aim to represent the likelihood and impact of risks in terms of the usual planning measures, such as time and money, according to Grey [10]. Qualitative risk management is easy to use. Quantitative risk management is more costly to implement but, provides more objective risk management than qualitative one.

The term risk management is applied in a number of diverse disciplines. People in the fields of statistics, economics, psychology, social sciences, biology, engineering,

toxicology, systems analysis, operations research, and decision theory, to name a few, have been addressing the field of risk management

Risk management consists of two steps, according to Fairley [9]:

- Risk Analysis
- Risk Control

Fairliy states that risk analysis involves the identification, evaluation, categorization, prioritization, and planning for mitigation of risks. This process begins with the start of the project and continues throughout the life of the project [9]. Parameters for evaluating, categorizing, and prioritizing risks include the followings according to Boehm [3]

- Risk probability
- Risk impact
- Thresholds to trigger management activities

Boehm mentions that risk control involves implementation of risk mitigation steps, close monitoring of the risks & identification of new risks, their mitigation etc. during the entire life cycle of the project [3].

2.2.1 Principles of Risk Management

There are principles for risk management to be performed effectively. According to Marvin, Suresh, and Ira, there are five principles given in Table 2 provide a framework to accomplish effective risk management for a typical software organization [20]. Kwak and Stoddard think the necessary principles for effective risk management as follows: [17]

- Shared Product Vision: A shared vision for success based upon commonality of purpose, shared ownersip, and collective commitment.
- Open Communications: A free flow of information at and between all program levels though formal, informal, and impromptu communication and consensus-based processes.
- System Percpective: That software development is viewed within the larger systems-level definition, design, and development.

- Proactive Strategies: Proactive strategies that involve planning and executing program activities based on anticipating future events.
- Systematic and Adaptable Methodolgy: A systematic approach that is adaptable to the program's infrastructure and culture.

Table 2 Risk Management Principles

Principle	**Effective risk management requires**
Global perspective	• Viewing software development within the context of the larger systems-level definition, design, and development • Recognizing both the potential value of opportunity and the potential impact of adverse effects.
Forward-looking view	• Thinking toward tomorrow, identifying uncertainties, anticipating potential outcomes • Managing project resources and activities while anticipating uncertainties.
Open communication	• Encouraging free-flowing information at and between all project levels. • Enabling formal, and informal communication. • Using processes that value the individual voice (bringing unique knowledge and insight to identifying and managing risk).
Integrated management	• Making risk management an integral and vital part of project management. • Adapting risk management methods and tools to a project's infrastructure and culture.
Continuous process	• Sustaining constant vigilance. • Identifying and managing risks routinely throughout all phases of the project's life cycle.

2.2.2 Functions of Risk Management

Higuera, and Dorofee's Risk Management Paradigm is depicted in Figure 1. The paradigm illustrates a set of functions that are identified as continuous activities throughout the life cycle of a project [12].

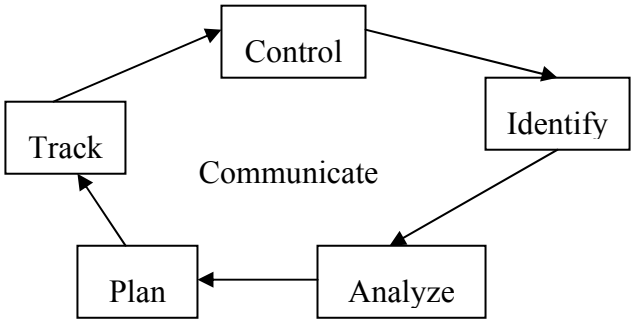

Figure 1 SEI Risk Management Paradigm

According to Higuera, and Dorofee, the functions of risk management are described in Table 3. Each risk nominally goes through these functions sequentially but the activity occurs continuously, concurrently, and iteratively throughout the project life cycle (e.g., planning for one risk may identify another) [12].

Table 3 Risk Management Functions

Function	**Description**
Identify	Search for and locate new risks before they become problems and adversely affect the program.
Analyze	Turn the raw risk data into decision-making information. Determine the values of impact, and likelihood. Set risk management priorities.
Plan	Translate risk information into decisions and actions (both present and future). Establish mitigation plans. Implement those actions.
Track	Monitor the status of risks and actions taken against risks.
Control	Correct for deviations from the planned risk actions.
Communicate	Provide information and feedback internal and external to the project on the risk activities, current risks, and emerging risks.

Risk identification is the first element in the risk management paradigm, according to Higuera, and Dorofee. Before risks can be managed, they must be identified. Risk identification aims to find the major risks before they adversely affect a program [12]. Chapman claims that identification is about the risk in proactive and reactive response terms [5].

Risk analysis is the next element in the risk management paradigm, according to Higuera, and Dorofee. Risk analysis is the conversion of risk data into risk

management information. Each risk must be understood sufficiently to allow a manager to make decisions. Risk analysis sets the known risks, and places the information in the hands of the decision maker. Analysis provides the information that allows managers to work on the right risks [12]. Khan, and Haddara states that "Risk analysis can be quantitative or qualitative. The output of a quantitative risk analysis will typically be a number, such as cost impact ($) per unit time. The number could be used to prioritize risk items. Quantitative risk analysis requires a great deal of data for both for the analysis of probabilities and analysis of consequences. Qualitative risk analysis is less rigorous and the results are often shown in the form of a simple matrix represents the probability and the other represents the consequences" [14]

Risk planning is needed after a risk is identified and analyzed, according to Higuera, and Dorofee. This element includes developing actions to address individual risks, prioritizing risk actions, and orchestrating the total risk management plan [12].

Risk tracking is required to ensure effective action plan implementation, according to Higuera, and Dorofee. This means that we must devise the risk metrics and triggering events needed to ensure that the planned risk actions are working. Tracking is the watch dog function of the risk action plan [12].

Risk control is the next element in the paradigm, according to Higuera, and Dorofee. Once the risk metrics and the triggering events have been chosen, there is nothing unique about risk management. Rather, risk management melds into program management and relies on program management processes to control the risk action plans, correct for variations from the plans, respond to triggering events, and improve the risk management process [12].

Finally, **risk communication** is at the center of the paradigm according to Higuera, and Dorofee; because, without effective communication, no risk management approach is viable. Communication is critical because it facilitates interaction among the elements of the paradigm. But there are higher level communications to consider as well. Risks must be communicated to the appropriate organizational levels so the risks can be analyzed and managed effectively [12].

According to Maude, and Willis, there are three parts to risk management as follows [21]:

1. Risk Identification: The first part of the risk management process is to know what the risks are [21].

2. Risk Analysis: Risk analysis takes the list of potential risk items, considers the probability of risk occurring, the expected losses if a risk does occur, and assesses the importance of each risk to the project [21].

3. Risk Control: Risk control takes the ordered risks, coordinates the resolution of these risks with the overall project plans, and monitors the project's progress towards resolving the risk items and meeting the goals [21].

Raz, and Michael think Risk Management methodolgy being consisted of Risk Identification, Risk Assessment, Risk Analysis, Risk Reduction and/or Mitigation, and Risk Monitoring [23].

Patterson, and Nealiey states seven steps of the project risk management areas follows [3]:

- Identify risk factors
- Assess risk probabilities and effects
- Develop strategies to mitigate identified risks
- Monitor risk factors
- Invoke a contingency plan
- Manage the crisis
- Recover from the crisis

2.3. Software Risk Management

Risks exist in software development for many reasons, according to Maude, and Willis [21]. Some of these are:

- It is difficult to determine the requirements

- The requirements may change during the development
- It is difficult to estimate costs and resources
- There is insufficient information at the start of development
- The development itself may have technical risks

Dedolph states that “Software risk management is risk management applied to the development and/or deployment of software-intensive systems” [6]. According to, Ropponen, and Lyytinen, software risk management is an approach that attempts to formalize risk oriented correlates of development success into a readily applicable set of principles and practices [25].

Ropponen, and Lyytinen believe that by including risk management in a project the exposure to software risk can be reduced and can thereby increase software quality and improve software development [25].

There is a methodology, to use in software risk management, called Risk Taxonomy. Ronald and Yacov offer a Risk Taxonomy methodology that follows the life cycle of software development and provides a framework for organizing data and information. The taxonomy-based identification method provides the organization developing software with a systematic interview process with which to identify sources of risk [24].

The taxonomy, offered by Ronald and Yacov, construct consists of a Taxonomy-Based Questionnaire and a process for its application (See Risk Classification paragraph, Appendix A, and Appendix B for detailed information about risk taxonomy). The taxonomy organizes software development risks into three levels: class, element, and attribute. The questionnaire consists of questions under each taxonomic attribute that are designed to elicit the range of risks and concerns potentially affecting the software product. The application process is designed such that the questionnaire can be used in a practical and efficient manner consistent with the objective of surfacing project risks. Both the questionnaire and the application process have been developed using extensive expertise and multiple field tests [24].

The taxonomy methodology, offered by Ronald and Yacov, is an instrument with which one can obtain a broad, system level of risks. These risks are commonly

identified by program members, and are classified by categories within the hierarchical structure of the taxonomy [24].

Ronald and Yacov's taxonomy of software development maps the characteristics of software development and software development risks. The questionnaire is a list of non-judgmental questions to elicit issues, concerns (i.e., potential risks), and risks in each taxonomic group. Hence, the questionnaire ensures that all risk areas are systematically addressed, while the application process is designed to ensure that the questions are asked of the right people and in the right manner to produce optimum results [24].

CHAPTER 3

DESCRIPTION AND CONDUCT OF THE STUDY

3.1. Methodology

The methodology used in this study is given in Figure 2.

3.1.1 Guide to Follow the Methodology

In order to provide an application study, data set should be defined at first. For this reason, the values of the parameters, defined in Figure 2, should be determined at first.

- Risk Identification: Two sources exist for risk identification in this study
    - Organization's risk database from the records in the organization (documented in Table 4)
    - Conduction of risk taxonomy to the organization from a team in the organization (documented in Table 5)
- Risk Classification: The classification in the technical report of 'CMU/SEI-93-TR-6' [29] is applied to whole set of risk items (documented in Table 6)
- Risk Probability: Defined risk probability ranges are applied to whole set of risk items (documented in Table 7)
    - The probability values for the risk items from the organization's risk database are converted to defined risk probability ranges
    - The probability values for the risk items identified by risk taxonomy are determined by a team in the organization

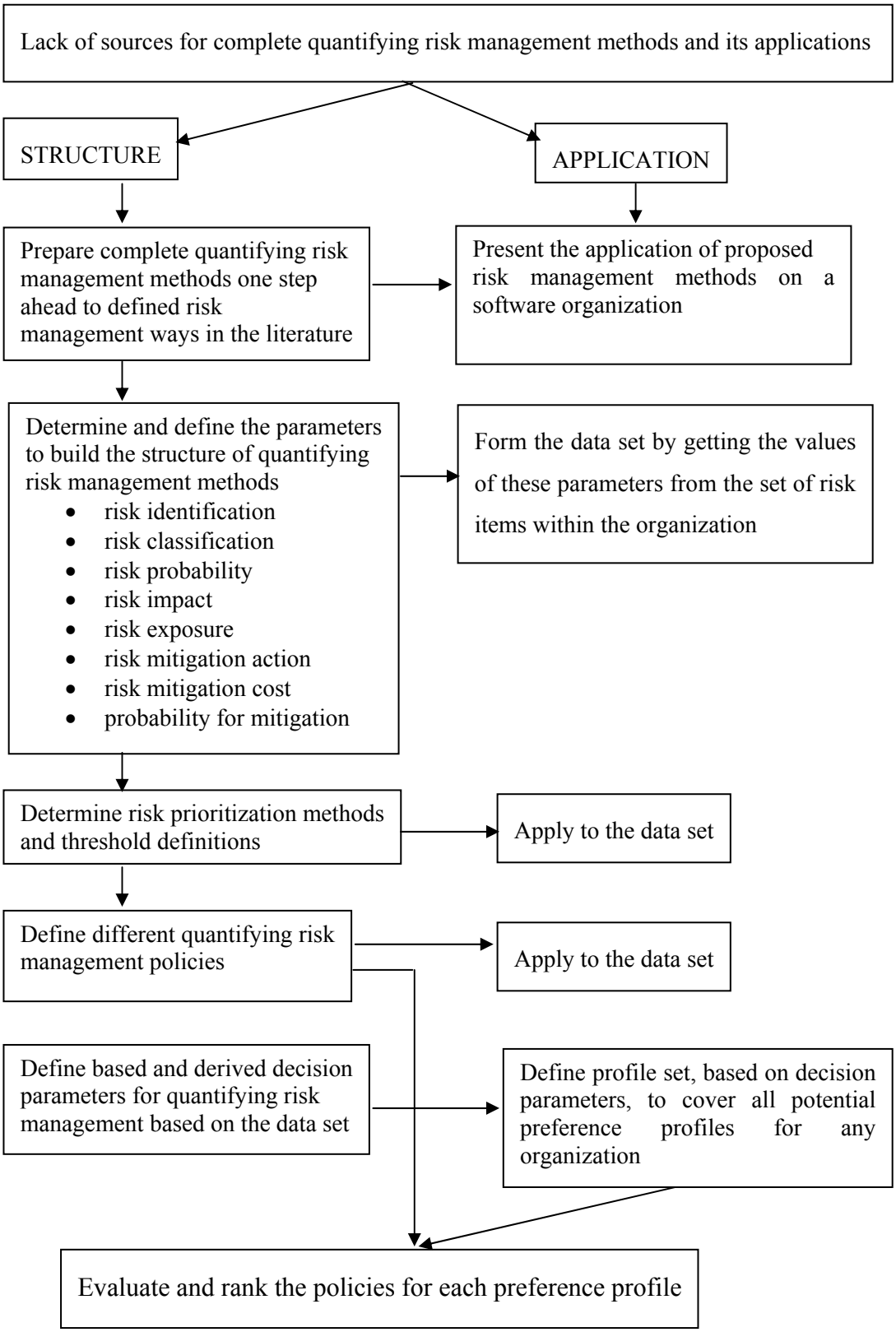

Figure 2 Methodology Flow Diagram

- Risk Impact: Defined risk impact ranges are applied to whole set of risk items (documented in Table 8)
    - The impact values for the risk items from the organization's risk database are converted to defined risk impact ranges
    - The impact values for the risk items identified by risk taxonomy are determined by a team in the organization
- Risk Exposure: Risk exposure values are calculated by the multiplication of risk probability value with risk impact value for whole set of risk items (documented in Table 11)
- Risk Mitigation Action: Risk mitigation actions are determined for whole set of risk items (documented in Table 12)
    - Risk mitigation actions for the risk items from the organization's risk database are available.
    - Risk mitigation actions for the risk items identified by risk taxonomy are determined by a team in the organization
- Risk Mitigation Cost: Risk mitigation costs for whole set of risk items are determined by a team in the organization (documented in Table 13).
- Probability for Mitigation: Probability for mitigation values for whole set of risk items are determined by a team in the organization (documented in Table 14).

Two main parameters to use in quantifying risk management are risk prioritization method, and threshold definition. Whole set of risk items are prioritized and sorted in accordance with determined risk prioritization method, and then determined threshold is applied to sorted risk items. Risk mitigation actions are applied to the risk items over threshold value, and monitoring for the risk items under threshold value.

Policies should be determined in order to use in quantifying risk management (documented in Table 15). Furthermore, profiles should be determined as covering maximum set of what an organization expects from quantifying risk management

(documented in Table 16). Policies are applied to data set. The results of the each policy in terms of decision parameters are analyzed (documented in Table 22-33).

Values of decision parameters are calculated for each policy in Table 17-19 (as summary of Table 22-33). In order to build Table 17-19, the content of the policies (given in Table 15) has been applied to data set.

At the end of the study, policies are ranked for each profile (documented in Table 20). An organization in a certain profile either could determine the most suitable policy for itself in terms of the results given or could apply its own data, and get most suitable policy for quantifying risk management for itself.

3.2. Description of the Method Applied in the Study

As shown in Chapter 2, the literature investigates various issues related to risk management and software risk management to find answers to following questions: What is the risk concept? What is the position of risk among opportunity, success, and problem? What is the scope of risk management and what it covers? Which principles provide a framework to accomplish effective risk management? What are the main functions of risk management? In addition to these, the literature also provides best practices for software risk management and its differences from risk management?

In the literature, there are sources for risk management. Some of them are qualitative, and some of them are quantitative. However, there is no much source about the application study of a quantifying risk management process on a software organization.

In order to obtain insight about this issue, this study presents a quantifying risk management system to the literature and also compares the quantifying risk management policies on the data set of a software organization by finding out and analyzing their performance with respect to designated decision parameters and preference profiles for risk items mitigated, exposures covered, costs, and expected exposures covered.

In this study, quantifying risk management are performed in accordance with the requirements of CMMI Maturity Level 3 [27]. The requirements put forward by CMMI for risk management and the solutions for these requirements are given at Chapter 5. Further, CMMI Maturity Level 3 (also called as 'Defined Level') enables the establishment of an infrastructure that institutionalizes effective software engineering and management processes across all projects [27]. By this way, all projects (in a maturity level 3 organization) operate according to procedures which are tailored from the standard processes put forward in the organizational level. This brings consistency among the process implementations performed by various projects. Hence, when this fact is considered together with the Risk Management Process Area's rules that each organization conforming to maturity level 3 shall comply with, designating the context of the study as CMMI enables the applicability of the potential results to many organizations. More clearly, the variability among the risk management implementations is minimized, since the considered software organizations conduct risk management according to Risk Management Process Area's rules of CMMI.

Besides of these, quantifying risk management in this study also cover the requirements of ISO 9001:2000 as shown at Chapter 5.

As described before, the aim of the study is to propose a quantifying risk management process and present its application on a software organization. In line with this aim, the study tries to have a set of risk items for risk analysis and risk control. In order to achieve this, the following information are gathered and analyzed in the rest of the study:

1. Risk Analysis
    - Risk Identification; to get the set of risk items covering the whole life cycle of any software organization
    - Risk Classification; to provide the classification of the identified risks
    - Risk Probability; to get the probability estimates for each identified risk
    - Risk Impact; to get the impact estimates for each identified risk
    - Risk Exposure; to calculate the exposure value for each identified risk
        i. Qualitative Method
        ii. Quantifying Method

2. Risk Control
    - Risk Mitigation Action; to define the mitigation action for each identified risk
    - Risk Mitigation Cost; to estimate the mitigation cost for each identified risk
    - Probability For Mitigation; to estimate the probability that mitigation action to prevent/reduce risk occurrence/exposure for each identified risk
    - Risk Prioritization Methods; to prioritize the risk items
        i. Prioritization Method 1
        ii. Prioritization Method 2
        iii. Prioritization Method 3
3. Thresholds
    - Definition of Thresholds; to monitor the risk items and to take action if any risk item exceeds the threshold
        i. Definition of Threshold 1
        ii. Definition of Threshold 2
        iii. Definition of Threshold 3

The data from my organization for these titles are gathered in this chapter, and analyzed in the next chapters.

3.3. Risk Analysis

3.3.1 Risk Identification

In risk identification, concern is paid for risk items being orthogonal. That means, no correlation between risk items and no interaction among risk items occur. The violation of this matter would cause the overestimation of risk items.

In this study, there are two sources for risk identification.

- Organization's current risk database. Risks are shown at Table 4. This database is formed by gathering the identified risk items of old/current projects.
- Conduct a risk assessment using a risk taxonomy. Risks are shown at Table 5. This database is formed by conduction of risk taxonomy to the old/current projects by a defined team in the organization.

Risk table by covering the risks coming from these two sources are built. Whole set of risk items are shown at Table 6.

Table 4 Organization's Current Risk Database

CLASS	ELEMENT	ATTRIBUTE	RISK ITEM
Product Engineering	Requirements	Stability	Requirements may not be defined on time and may be changed after the approval of requirements document
Product Engineering	Requirements	Completeness	Current System Requirements are not well-defined, and some system requirements may be caught
Product Engineering	Requirements	Validity	X module has been positioned wrongly in the project. There may be lack of system requirements for AVINT that is not included in the contract
Product Engineering	Design	Difficulty	Taking of risky design decisions in terms of project schedule and personnel number
Product Engineering	Design	Interfaces	Possibility of interface conflicts in the system design
Product Engineering	Integration and Test	Product	There may be deviations from test results because of integration of unfinished CSCIs coming from Prime Contractor
Product Engineering	Integration and Test	System	Leaving of some works after acceptance tests due to reasons not from STM
Product Engineering	Integration and Test	System	High percentage of defects occurring in system acceptance tests/Risk of customer unsatisfaction
Product Engineering	Integration and Test	System	Planning some activities is nearly impossible because integration and acceptance process is not clear
Development Environment	Development Process	Formality	The lack of standardized unit test descriptions and test methods in the organization
Development Environment	Development System	Usability	Providing of Software Integration Environment by customer may not be performed
Development Environment	Development System	Reliability	Risk of video quality being low
Development Environment	Development System	System Support	HA and VTE simulators are needed for more efficiency in the Software Development Activities. These simulators may not be provided
Development Environment	Development System	System Support	Needed CSCI versions may not be provided from Prime Contractor to use in software tests
Development Environment	Management Process	Planning	Preparation of related documents for Avionic Emulator that are covered in contract but not covered in Work Breakdown Structure

Table 4 Organization's Current Risk Database (cont'd)

Program Constraints	Resources	Schedule	The allocated time for development phase is not sufficient
Program Constraints	Resources	Staff	Leaving of project personnel/Being late for inefficient performance of the project personnel
Program Constraints	Resources	Staff	Leaving of project personnel during development phases
Program Constraints	Resources	Budget	Some requirements may need more effort than estimated
Program Constraints	Contract	Restrictions	Work definitions that are not covered in contract may be performed
Program Constraints	Contract	Restrictions	New user requirements that are not covered in the contract
Program Constraints	Program Interfaces	Customer	Change requests for document context from the customer
Program Constraints	Program Interfaces	Customer	Requirements may be changed, added or deleted. That may affect the project's schedule and context
Program Constraints	Program Interfaces	Customer	CDR meeting and necessary approval may be late
Program Constraints	Program Interfaces	Customer	Data provided by customer according to contract, may be provided late
Program Constraints	Program Interfaces	Customer	MFD hardware provided by customer according to contract, may be provided late
Program Constraints	Program Interfaces	Associate Contractors	Prime Contractor may give design decisions after baselined design document. That may lead to loss of effort in organization
Program Constraints	Program Interfaces	Prime Contractor	Preparation of Software Design Descriptions may delay and that's why, coding activities may be in difficulty
Program Constraints	Program Interfaces	Prime Contractor	A need may occur for CBS licensing from Prime Contractor
Program Constraints	Program Interfaces	Prime Contractor	Late comment from Prime Contractor for test documents, and change request for test documents during performing tests
Program Constraints	Program Interfaces	Politics	Answer/approval time may be late because of conflicts between customer, users, and associated contractors.
Program Constraints	Program Interfaces	Politics	Project may be cancelled by government because of its high budget, and conflicts between contractors

Table 5 Organization's Risks Using a Risk Taxonomy

CLASS	ELEMENT	ATTRIBUTE	RISK ITEM
Product Engineering	Requirements	Stability	Requirements are changing and new requirements are added although requirement document is baselined. So, final delivery on time is getting harder because of changed and new requirements.
Product Engineering	Requirements	Stability	Customer introducing new system requirements without budget or schedule relief this is muddying the project's lines of authority
Product Engineering	Requirements	Completeness	Incomplete requirements specification due to an uncertain customer
Product Engineering	Requirements	Completeness	There are some TBDs "To Be Determined" in requirement specification document. These TBDs should be determined before the release of requirement specification document.
Product Engineering	Requirements	Clarity	Some requirements are not clear to fully understand, and may lead to wrong interpretation.
Product Engineering	Requirements	Validity	Development of extra software functions that are not required (gold-plating) extends the schedule
Product Engineering	Requirements	Validity	Customer does not have a solid idea of what is required, and think to have unwritten requirements/expectations. (prototype, These requirements should be able to be captured into the system as soon as possible)
Product Engineering	Requirements	Precedent	Requirements demand the use of new analysis, design or testing methods.
Product Engineering	Requirements	Precedent	Technology for this project is new to organization. Organization does not have sufficient knowledge in this area (plan for acquiring knowledge, hiring people, training)
Product Engineering	Design	Functionality	Inappropriate design solution leads to redesign and reimplementation
Product Engineering	Design	Difficulty	Design solutions are not selected by objective evaluation, so it may be difficult to have solutions for all the requirements. (process for objective solution)
Product Engineering	Design	Interfaces	Developing the wrong user interface
Product Engineering	Design	Interfaces	Interdependency commitments might change without everyone being informed, and that might result in interface defects

Table 5 Organization's Risks Using a Risk Taxonomy (cont'd)

Product Engineering	Design	Interfaces	System interface information may not be provided on time and that is why, product delivery may be late
Product Engineering	Design	Interfaces	Software builds with interface with vendor supplied software products that are unproven
Product Engineering	Design	Interfaces	Product will be used with hardware, but the interfaces of the software with the hardware are not well defined yet.
Product Engineering	Design	Performance	Size of Ada executable and slow execution may exceed hardware and timing limitations
Product Engineering	Design	Testability	Testers have not involved in analyzing requirements
Product Engineering	Design	Hardware Constraints	RISC based hardware shall be used in the project. This technology is not well known by project the personnel. That is why, software development activities may be late
Product Engineering	Code and Unit Test	Testing	Because of tight schedule, sufficient unit testing is not performed
Product Engineering	Code and Unit Test	Coding /Implementation	There is a lack of experienced C programmers, code may be inefficient//late
Product Engineering	Code and Unit Test	Coding /Implementation	Design specifications are not in sufficient detail to write the code.
Product Engineering	Integration and Test	Environment	During the establishment of test environment, the selection of the configuration items with correct revisions is not checked, so risk for selecting wrong revisions for testing
Product Engineering	Integration and Test	Environment	The software ordered for testing the system may be delayed due to a "backorder" status resulting schedule change to a critical path activity
Product Engineering	Integration and Test	Product	Just in time delivery of software will result in too-little time to integrate and field fix defects (Establish requirements)
Product Engineering	Integration and Test	Product	There is only limited time for testing
Product Engineering	Integration and Test	System	All contractors are not part of the integration team
Product Engineering	Integration and Test	System	Integrated testing dependent upon multiple activity. Testing may fail

Table 5 Organization's Risks Using a Risk Taxonomy (cont'd)

Product Engineering	Engineering Specialities	Maintainability	Maintenance people are not involved early in the design, because maintenance planning is not performed before.
Product Engineering	Engineering Specialities	Maintainability	Design is not performed by considering maintenance expectations.
Product Engineering	Engineering Specialities	Security	Organization ahs not implemented this level of security before.
Product Engineering	Engineering Specialities	Human Factors	The design related with human/user interfaces of the product may not be as what the user wants.
Product Engineering	Engineering Specialities	Specifications	Project manager is undercut and new requirements are introduced: these may remain hidden and no test cases will be developed for them
Development Environment	Development Process	Suitability	Inaccurate metrics may cause to wrong interpretation of process performances
Development Environment	Development Process	Process Control	Some written processes may not be followed
Development Environment	Development Process	Process Control	Development processes in not well measured to evaluate the meeting of productivity and quality goals.
Development Environment	Development Process	Familiarity	Some new developers are not familiar with development processes and plans.
Development Environment	Development Process	Product Control	New requirements are added to the system but adequate analysis is not performed
Development Environment	Development System	Capacity	We have never tried to make 10 computers work together like this; it could delay final system acceptance
Development Environment	Development System	Usability	Some documentations coming from prime contractors are in different format than ours. Traceability may be difficult between documents in two different formats.
Development Environment	Development System	Familiarity	Technology to be built is new to the organization
Development Environment	Development System	Familiarity	Operation in an unfamiliar or unproved software environment causes unforeseen problems
Development Environment	Development System	Reliability	Loss of data during conversation from one system to another
Development Environment	Management Process	Planning	Estimation is not based on historical data
Development Environment	Management Process	Planning	Planning is not based on experienced estimation process. So, no reliable effort estimate

Table 5 Organization's Risks Using a Risk Taxonomy (cont'd)

Development Environment	Management Process	Planning	People at all levels are not included in planning their own work
Development Environment	Management Process	Program Interfaces	Customer is not willing to participate in reviews
Development Environment	Management Process	Program Interfaces	No real cooperation between contractors
Development Environment	Management Process	Program Interfaces	It takes too long to resolve issues with the customer. Customer approval of deliverable documentation content (CDRL) is too long.
Development Environment	Management Process	Program Interfaces	Because of more than one contractor, the solution of the some problems can be time consuming.
Development Environment	Management Methods	Monitoring	Some collected process metrics are not evaluated, so project managers cannot be informed about the performance of the processes.
Development Environment	Management Methods	Personnel Management	Staff have not received enough training in some areas
Development Environment	Management Methods	Personnel Management	Yearly holiday of the personnel may be overlapped, and some works may not be performed within a certain schedule.
Development Environment	Management Methods	Configuration Management	New CM tool is applied, Problems may occur during usage
Development Environment	Management Methods	Configuration Management	CM staff is not experienced, and CM tool is not used efficiently.
Development Environment	Work Environment	Cooperation	During choosing design solution out of alternatives, the owners of the unchosen alternatives may not trust on the chosen alternative and may show lack of cooperation.
Development Environment	Work Environment	Cooperation	Interdependency commitments might change without everyone being informed, and that might result in interface defects.
Program Constraints	Resources	Schedule	Schedule is not planned for trainings, so deviation from schedule can occur.
Program Constraints	Resources	Schedule	Schedule is optimistic, "best case," rather than realistic, "expected case"
Program Constraints	Resources	Schedule	Excessive schedule pressure reduces productivity

Table 5 Organization's Risks Using a Risk Taxonomy (cont'd)

Program Constraints	Resources	Schedule	Schedule is based on estimation but estimation is performed a bit subjective (depends on the performer) not based on historical data. So, schedule may not be the deserved schedule.
Program Constraints	Resources	Staff	Staff in configuration management is not experienced, that may affect the success of the project.
Program Constraints	Resources	Staff	Adding personnel to a late project
Program Constraints	Resources	Staff	Staffing may be not stable because of external factors like personal allocation to other projects, or personnel to leave the job
Program Constraints	Resources	Budget	Current availability leaves no time to correct potential defects found occurring aboard new product.
Program Constraints	Contract	Type of Contract	Approval cycle for required documentation is long. This affects the performing of other work on time.
Program Constraints	Contract	Dependencies	The cases for adding/changing/deleting requirements are not defined in the contract. So, actions related with requirements may affect the success of project.
Program Constraints	Program Interfaces	Customer	Customer does not understand technical aspects of the system well, so specifications may change any time after customer approval
Program Constraints	Program Interfaces	Customer	Customer who care less for the process but is interested only in the final product. This may cause the problem in the customer related process
Program Constraints	Program Interfaces	Customer	Insufficient training of end user
Program Constraints	Program Interfaces	Prime Contractor	We are highly dependent to Prime Contractor for getting test tool, if test tool delays then schedule also delays

Table 6 Organization's Whole Set of Risks

CLASS	ELEMENT	ATTRIBUTE	RISK NO	RISK ITEM
Product Engineering	Requirements	Stability	1	Requirements are changing and new requirements are added although requirement document is baselined. So, final delivery on time is getting harder because of changed and new requirements.
Product Engineering	Requirements	Stability	2	Requirements may not be defined on time and may be changed after the approval of requirements document
Product Engineering	Requirements	Stability	3	Customer introducing new system requirements without budget or schedule relief this is muddying the project's lines of authority
Product Engineering	Requirements	Completeness	4	Incomplete requirements specification due to an uncertain customer
Product Engineering	Requirements	Completeness	5	Current System Requirements are not well-defined, and some system requirements may be caught
Product Engineering	Requirements	Completeness	6	There are some TBDs "To Be Determined" in requirement specification document. These TBDs should be determined before the release of requirement specification document.
Product Engineering	Requirements	Clarity	7	Some requirements are not clear to fully understand, and may lead to wrong interpretation.
Product Engineering	Requirements	Validity	8	Development of extra software functions that are not required (gold-plating) extends the schedule
Product Engineering	Requirements	Validity	9	X module has been positioned wrongly in the project. There may be lack of system requirements for AVINT that is not included in the contract
Product Engineering	Requirements	Validity	10	Customer does not have a solid idea of what is required, and think to have unwritten requirements/expectations.
Product Engineering	Requirements	Precedent	11	Requirements demand the use of new analysis, design or testing methods.
Product Engineering	Requirements	Precedent	12	Technology for this project is new to organization. Organization does not have sufficient knowledge in this area

Table 6 Organization's Whole Set of Risks (cont'd)

Product Engineering	Design	Functionality	13	Inappropriate design solution leads to redesign and reimplementation
Product Engineering	Design	Difficulty	14	Taking of risky design decisions in terms of project schedule and personnel number
Product Engineering	Design	Difficulty	15	Design solutions are not selected by objective evaluation, so it may be difficult to have solutions for all the requirements.
Product Engineering	Design	Interfaces	16	Developing the wrong user interface
Product Engineering	Design	Interfaces	17	Interdependency commitments might change without everyone being informed, and that might result in interface defects
Product Engineering	Design	Interfaces	18	System interface information may not be provided on time and that is why, product delivery may be late
Product Engineering	Design	Interfaces	19	Possibility of interface conflicts in the system design
Product Engineering	Design	Interfaces	20	Software builds with interface with vendor supplied software products that are unproven
Product Engineering	Design	Interfaces	21	Product will be used with hardware, but the interfaces of the software with the hardware are not well defined yet.
Product Engineering	Design	Performance	22	Size of Ada executable and slow execution may exceed hardware and timing limitations
Product Engineering	Design	Testability	23	Testers have not involved in analyzing requirements
Product Engineering	Design	Hardware Constraints	24	RISC based hardware shall be used in the project. This technology is not well known by project the personnel. That is why, software development activities may be late
Product Engineering	Code and Unit Test	Testing	25	Because of tight schedule, sufficient unit testing is not performed
Product Engineering	Code and Unit Test	Coding/ Implementation	26	There is a lack of experienced C programmers, code may be inefficient/late
Product Engineering	Code and Unit Test	Coding/ Implementation	27	Design specifications are not in sufficient detail to write the code.

Table 6 Organization's Whole Set of Risks (cont'd)

Product Engineering	Integration and Test	Environment	28	During the establishment of test environment, the selection of the configuration items with correct revisions is not checked, so risk for selecting wrong revisions for testing
Product Engineering	Integration and Test	Environment	29	The software ordered for testing the system may be delayed due to a "backorder" status resulting schedule change to a critical path activity
Product Engineering	Integration and Test	Product	30	Just in time delivery of software will result in too-little time to integrate and field fix defects
Product Engineering	Integration and Test	Product	31	There may be deviations from test results because of integration of unfinished CSCIs coming from Prime Contractor
Product Engineering	Integration and Test	Product	32	There is only limited time for testing
Product Engineering	Integration and Test	System	33	All contractors are not part of the integration team
Product Engineering	Integration and Test	System	34	Integrated testing dependent upon multiple activity. Testing may fail
Product Engineering	Integration and Test	System	35	Leaving of some works after acceptance tests due to reasons not from STM
Product Engineering	Integration and Test	System	36	High percentage of defects occurring in system acceptance tests/Risk of customer unsatisfaction
Product Engineering	Integration and Test	System	37	Planning some activities is nearly impossible because integration and acceptance process is not clear.
Product Engineering	Engineering Specialities	Maintainability	38	Maintenance people are not involved early in the design, because maintenance planning is not performed before.
Product Engineering	Engineering Specialities	Maintainability	39	Design is not performed by considering maintenance expectations.
Product Engineering	Engineering Specialities	Security	40	Organization has not implemented this level of security before.
Product Engineering	Engineering Specialities	Human Factors	41	The design related with human/user interfaces of the product may not be as what the user wants.
Product Engineering	Engineering Specialities	Specifications	42	Project manager is undercut and new requirements are introduced: these may remain hidden and no test cases will be developed for them

Table 6 Organization's Whole Set of Risks (cont'd)

Development Environment	Development Process	Formality	43	The lack of standardized unit test descriptions and test methods in the organization
Development Environment	Development Process	Suitability	44	Inaccurate metrics may cause to wrong interpretation of process performances
Development Environment	Development Process	Process Control	45	Some written processes may not be followed
Development Environment	Development Process	Process Control	46	Development processes are not well measured to evaluate the meeting of productivity and quality goals.
Development Environment	Development Process	Familiarity	47	Some new developers are not familiar with development processes and plans.
Development Environment	Development Process	Product Control	48	New requirements are added to the system but adequate analysis is not performed
Development Environment	Development System	Capacity	49	We have never tried to make 10 computers work together like this; it could delay final system acceptance
Development Environment	Development System	Usability	50	Providing of Software Integration Environment by customer may not be performed
Development Environment	Development System	Usability	51	Some documentations coming from prime contractors are in different format than ours. Traceability may be difficult between documents in two different formats.
Development Environment	Development System	Familiarity	52	Technology to be built is new to the organization
Development Environment	Development System	Familiarity	53	Operation in an unfamiliar or unproved software environment causes unforeseen problems
Development Environment	Development System	Reliability	54	Risk of video quality being low
Development Environment	Development System	Reliability	55	Loss of data during conversation from one system to another
Development Environment	Development System	System Support	56	HA and VTE simulators are needed for more efficiency in the Software Development Activities. These simulators may not be provided
Development Environment	Development System	System Support	57	Needed CSCI versions may not be provided from Prime Contractor to use in software tests
Development Environment	Management Process	Planning	58	Estimation is not based on historical data

Table 6 Organization's Whole Set of Risks (cont'd)

Development Environment	Management Process	Planning	59	Preparation of related documents for Avionic Emulator that are covered in contract but not covered in Work Breakdown Structure
Development Environment	Management Process	Planning	60	Planning is not based on experienced estimation process. So, no reliable effort estimate
Development Environment	Management Process	Planning	61	People at all levels are not included in planning their own work
Development Environment	Management Process	Program Interfaces	62	Customer is not willing to participate in reviews
Development Environment	Management Process	Program Interfaces	63	No real cooperation between contractors
Development Environment	Management Process	Program Interfaces	64	It takes too long to resolve issues with the customer. Customer approval of deliverable documentation content (CDRL) is too long.
Development Environment	Management Process	Program Interfaces	65	Because of more than one contractor, the solution of the some problems can be time consuming.
Development Environment	Management Methods	Monitoring	66	Some collected process metrics are not evaluated, so project managers may not be informed about the performance of the processes.
Development Environment	Management Methods	Personnel Management	67	Staff have not received enough training in some areas
Development Environment	Management Methods	Personnel Management	68	Yearly holiday of the personnel may be overlapped, and some works may not be performed within a certain schedule.
Development Environment	Management Methods	Configuration Management	69	New CM tool is applied, Problems may occur during usage
Development Environment	Management Methods	Configuration Management	70	CM staff is not experienced, and CM tool is not used efficiently.
Development Environment	Work Environment	Cooperation	71	During choosing design solution out of alternatives, the owners of the unchosen alternatives may not trust on the chosen alternative and may show lack of cooperation.
Program Constraints	Resources	Schedule	72	Schedule is not planned for trainings, so deviation from schedule can occur.
Program Constraints	Resources	Schedule	73	The allocated time for development phase is not sufficient

Table 6 Organization's Whole Set of Risks (cont'd)

Program Constraints	Resources	Schedule	74	Schedule is optimistic, "best case," rather than realistic, "expected case"
Program Constraints	Resources	Schedule	75	Excessive schedule pressure reduces productivity
Program Constraints	Resources	Schedule	76	Schedule is based on estimation but estimation is performed a bit subjective (depends on the performer) not based on historical data. So, schedule may not be the deserved schedule.
Program Constraints	Resources	Staff	77	Staff in configuration management is not experienced, that may affect the success of the project.
Program Constraints	Resources	Staff	78	Leaving of project personnel/Being late for inefficient performance of the project personnel
Program Constraints	Resources	Staff	79	Leaving of project personnel during development phases
Program Constraints	Resources	Staff	80	Adding personnel to a late project
Program Constraints	Resources	Staff	81	Staffing may be not stable because of external factors like personal allocation to other projects, or personnel to leave the job
Program Constraints	Resources	Budget	82	Some requirements may need more effort than estimated
Program Constraints	Resources	Budget	83	Current availability leaves no time to correct potential defects found occurring aboard new product.
Program Constraints	Contract	Type of Contract	84	Approval cycle for required documentation is long. This affects the performing of other works.
Program Constraints	Contract	Restrictions	85	Work definitions that are not covered in contract may be performed
Program Constraints	Contract	Restrictions	86	New user requirements that are not covered in the contract
Program Constraints	Contract	Dependencies	87	The cases for adding/changing/deleting requirements are not defined in the contract. So, actions related with requirements may affect the success of project.
Program Constraints	Program Interfaces	Customer	88	Customer does not understand technical aspects of the system well, so specifications may change any time after customer approval

Table 6 Organization's Whole Set of Risks (cont'd)

Program Constraints	Program Interfaces	Customer	89	Customer who care less for the process but is interested only in the final product. This may cause the problem in the customer related process
Program Constraints	Program Interfaces	Customer	90	Insufficient training of end user
Program Constraints	Program Interfaces	Customer	91	Change requests for document context from the customer
Program Constraints	Program Interfaces	Customer	92	Requirements may be changed, added or deleted. That may affect the project's schedule and context
Program Constraints	Program Interfaces	Customer	93	CDR meeting and necessary approval may be late
Program Constraints	Program Interfaces	Customer	94	Data provided by customer according to contract, may be provided late
Program Constraints	Program Interfaces	Customer	95	MFD hardware provided by customer according to contract, may be provided late
Program Constraints	Program Interfaces	Associate Contractors	96	Prime Contractor may give design decisions after baselined design document. That may lead to loss of effort in organization
Program Constraints	Program Interfaces	Prime Contractor	97	We are highly dependent to Prime Contractor for getting test tool, if test tool delays then schedule also delays
Program Constraints	Program Interfaces	Prime Contractor	98	Preparation of Software Design Descriptions may delay and that's why, coding activities may be in difficulty
Program Constraints	Program Interfaces	Prime Contractor	99	A need may occur for CBS licensing from Prime Contractor
Program Constraints	Program Interfaces	Prime Contractor	100	Late comment from Prime Contractor for test documents, and change request for test documents during performing tests
Program Constraints	Program Interfaces	Politics	101	Answer/approval time may be late because of conflicts between customer, users, and associated contractors.
Program Constraints	Program Interfaces	Politics	102	Project may be cancelled by government because of its high budget, and conflicts between contractors

3.3.2 Risk Classification

Establishing classifications for risks provides a mechanism for collecting and organizaing risks.

Current risk classification in the organization combined of ‘technicacal risks’ and ‘managerial risks’. This classification is not sufficient and not defined well. So, it can be improved.

Risk classification of each risk item are based on the risk taxonomy classes. The software taxonomy is organized into three major classes. These are

1. **Product Engineering**: The technical aspects of the work to be accomplished.
2. **Development Environment**: The methods, procedures, and tools used to produce the product.
3. **Program Constraints**: The contractual, organizational, and operational factors within which the software is developed but which are generally outside of the direct control of the local management.

These classes consist of sub-classes mentioned below:

1. **Product Engineering**
    a. Requirements
        i. Stability
        ii. Completeness
        iii. Clarity
        iv. Validity
        v. Feasibility
        vi. Precedent
        vii. Scale
    b. Design
        i. Functionality
        ii. Difficulty
        iii. Interfaces
        iv. Performance
        v. Testability
        vi. Hardware Constraints
        vii. Non-developmental Software
    c. Code and Unit Test
        i. Feasibility
        ii. Testing
        iii. Coding/Implementation
    d. Integration and Test
        i. Environment
        ii. Product

iii. System
e. Engineering Specialities
i. Maintainability
ii. Reliability
iii. Safety
iv. Security
v. Human Factors
vi. Specifications

2. Development Environment

a. Development Process
i. Formality
ii. Suitability
iii. Process Control
iv. Familarity
v. Product Control
b. Development System
i. Capacity
ii. Suitability
iii. Usability
iv. Familarity
v. Reliability
vi. System Support
vii. Deliverability
c. Management Process
i. Planning
ii. Project Organization
iii. Management Experience
iv. Program Interfaces
d. Management Methods
i. Monitoring
ii. Personel Management
iii. Quality Assurance
iv. Configuration Management
e. Work Environment
i. Quality Attitude
ii. Cooperation
iii. Communication
iv. Morale

3. Program Constraints

a. Resources
i. Schedule
ii. Staff
iii. Budget
iv. Facilities
b. Contract
i. Type of Contract
ii. Restrictions
iii. Dependencies

c. Program Interfaces
    i. Customer
    ii. Associate Conractors
    iii. Subcontractors
    iv. Prime Contractor
    v. Corporate Management
    vi. Vendors
    vii. Politics

The detailed information of the each class/sub-class and its concept are given in Appendix A.

The overall distrubition of all the risks (given in Table 6) in the organization within these three classes indicates a nearly even decision:

- 42 % Product Engineering (= 42/102, 42 risk items within Product Engineering class, 102 risk items for whole set)
- 28 % Development Environment (= 29/102, 29 risk items within Development Environment class, 102 risk items for whole set)
- 30 % Program Constraints (= 31/102, 31 risk items within Program Constraints class, 102 risk items for whole set)

Below is a summary of the distribution of risks associated with each sub level of the taxonomy hierarchy in our organization:

Major Elements of Risk Within Each Class

Of the five subcategories of risk within product engineering in Table 6

- Requirements scored 29 % of all risks (= 12/42, 12 risk items within Requirements element, 42 risk items for Product Engineering class)
- Design scored 29 % of all risks (= 12/42, 12 risk items within Design element, 42 risk items for Product Engineering class)
- Integration and Test scored 23 % of all risks (= 10/42, 10 risk items within Integration and Test element, 42 risk items for Product Engineering class)
- Engineering Specialities scored 12 % of all risks (= 5/42, 5 risk items within Engineering Specialities element, 42 risk items for Product Engineering class)
- Code and Unit Test scored 7 % of all risks (= 3/42, 3 risk items within Code and Unit Test element, 42 risk items for Product Engineering class)

These results are not surprising, because they confirm the notion that within product engineering, about 60 % of all risks are attributed to Requirements and Design.

Of the five subcategories of risk within development environment in Table 6

- Development Process scored 20 % of all risks (= 6/29, 6 risk items within Development Process element, 29 risk items for Development Environment class)
- Development System scored 31 % of all risks (= 9/29, 9 risk items within Development System element, 29 risk items for Development Environment class)
- Management Process scored 28 % of all risks (= 8/29, 8 risk items within Management Process element, 29 risk items for Development Environment class)
- Management Methods scored 17 % of all risks (= 5/29, 5 risk items within Management Methods element, 29 risk items for Development Environment class)
- Work Environment scored 4 % of all risks (= 1/29, 1 risk item within Work Environment element, 29 risk items for Development Environment class)

These statistics confirm that development system, and management process are critically important in meeting development requirements.

Of the five subcategories of risk within program constraints in Table 6

- Resources scored 39 % of all risks (= 12/31, 12 risk items within Resources element, 31 risk items for Program Constraints class)
- Contract scored 13 % of all risks (= 4/31, 4 risk items within Resources element, 31 risk items for Program Constraints class)
- Program Interfaces scored 48 % of all risks (= 15/31, 15 risk items within Program Interfaces element, 31 risk items for the Program Constraints class)

About half of all sources of risks in Program Constraints are attributed to Program Interfaces.

3.3.3 Risk Probability

Risk probability is the likelihood that the concequence of a risk will be realized given that the current situation is allowed to continue. In other words, how likely is the problem to actually occur.

Risk probability for each of the risk item is assigned subjectively by the organization. Probability of occurrence for each risk item is assigned in the range of '0 – 1.0'. In this study, certain values used for risk probability are assumed as the followings by the organization:

- impossible – 0 (this is not risk)
- remote – 0.1
- unlikely – 0.3

- likely – 0.5
- highly likely – 0.7
- very likely – 0.9
- certain – 1.0 (this is problem, not a risk)

According to these values, subjective probability estimates for the risk items are shown in Table 7.

Table 7 Organization's Risks with Probability Estimates

RISK NO	RISK ITEM	Probability
1	Requirements are changing and new requirements are added although requirement document is baselined. So, final delivery on time is getting harder because of changed and new requirements.	0.7
2	Requirements may not be defined on time and may be changed after the approval of requirements document	0.5
3	Customer introducing new system requirements without budget or schedule relief this is muddying the project's lines of authority	0.3
4	Incomplete requirements specification due to an uncertain customer	0.5
5	Current System Requirements are not well-defined, and some system requirements may be caught	0.7
6	There are some TBDs "To Be Determined" in requirement specification document. These TBDs should be determined before the release of requirement specification document.	0.7
7	Some requirements are not clear to fully understand, and may lead to wrong interpretation.	0.3
8	Development of extra software functions that are not required (gold-plating) extends the schedule	0.1
9	X module has been positioned wrongly in the project. There may be lack of system requirements for AVINT that is not included in the contract	0.5
10	Customer does not have a solid idea of what is required, and think to have unwritten requirements/expectations.	0.7
11	Requirements demand the use of new analysis, design or testing methods.	0.3
12	Technology for this project is new to organization. Organization does not have sufficient knowledge in this area	0.3
13	Inappropriate design solution leads to redesign and reimplementation	0.5
14	Taking of risky design decisions in terms of project schedule and personnel number	0.5
15	Design solutions are not selected by objective evaluation, so it may be difficult to have solutions for all the requirements.	0.7
16	Developing the wrong user interface	0.3
17	Interdependency commitments might change without everyone being informed, and that might result in interface defects	0.1

Table 7 Organization's Risks with Probability Estimates (cont'd)

18	System interface information may not be provided on time and that is why, product delivery may be late	0.3
19	Possibility of interface conflicts in the system design	0.5
20	Software builds with interface with vendor supplied software products that are unproven	0.5
21	Product will be used with hardware, but the interfaces of the software with the hardware are not well defined yet.	0.7
22	Size of Ada executable and slow execution may exceed hardware and timing limitations	0.3
23	Testers have not involved in analyzing requirements	0.7
24	RISC based hardware shall be used in the project. This technology is not well known by project the personnel. That is why, software development activities may be late	0.5
25	Because of tight schedule, sufficient unit testing is not performed	0.9
26	There is a lack of experienced C programmers, code may be inefficient/late	0.5
27	Design specifications are not in sufficient detail to write the code.	0.3
28	During the establishment of test environment, the selection of the configuration items with correct revisions is not checked, so risk for selecting wrong revisions for testing	0.3
29	The software ordered for testing the system may be delayed due to a "backorder" status resulting schedule change to a critical path activity	0.3
30	Just in time delivery of software will result in too-little time to integrate and field fix defects	0.3
31	There may be deviations from test results because of integration of unfinished CSCIs coming from Prime Contractor	0.5
32	There is only limited time for testing	0.7
33	All contractors are not part of the integration team	0.7
34	Integrated testing dependent upon multiple activity. Testing may fail	0.5
35	Leaving of some works after acceptance tests due to reasons not from STM	0.5
36	High percentage of defects occurring in system acceptance tests/Risk of customer unsatisfaction	0.5
37	Planning some activities is nearly impossible because integration and acceptance process is not clear	0.7
38	Maintenance people are not involved early in the design, because maintenance planning is not performed before.	0.7
39	Design is not performed by considering maintenance expectations.	0.7

Table 7 Organization's Risks with Probability Estimates (cont'd)

40	Organization has not implemented this level of security before.	0.3
41	The design related with human/user interfaces of the product may not be as what the user wants.	0.3
42	Project manager is undercut and new requirements are introduced: these may remain hidden and no test cases will be developed for them	0.3
43	The lack of standardized unit test descriptions and test methods in the organization	0.5
44	Inaccurate metrics may cause to wrong interpretation of process performances	0.5
45	Some written processes may not be followed	0.3
46	Development processes are not well measured to evaluate the meeting of productivity and quality goals.	0.5
47	Some new developers are not familiar with development processes and plans.	0.7
48	New requirements are added to the system but adequate analysis is not performed	0.5
49	We have never tried to make 10 computers work together like this; it could delay final system acceptance	0.7
50	Providing of Software Integration Environment by customer may not be performed	0.3
51	Some documentations coming from prime contractors are in different format than ours. Traceability may be difficult between documents in two different formats.	0.3
52	Technology to be built is new to the organization	0.3
53	Operation in an unfamiliar or unproved software environment causes unforeseen problems	0.7
54	Risk of video quality being low	0.5
55	Loss of data during conversation from one system to another	0.3
56	HA and VTE simulators are needed for more efficiency in the Software Development Activities. These simulators may not be provided	0.5
57	Needed CSCI versions may not be provided from Prime Contractor to use in software tests	0.5
58	Estimation is not based on historical data	0.7
59	Preparation of related documents for Avionic Emulator that are covered in contract but not covered in Work Breakdown Structure	0.9
60	Planning is not based on experienced estimation process. So, no reliable effort estimate	0.7
61	People at all levels are not included in planning their own work	0.5
62	Customer is not willing to participate in reviews	0.7

Table 7 Organization's Risks with Probability Estimates (cont'd)

63	No real cooperation between contractors	0.7
64	It takes too long to resolve issues with the customer. Customer approval of deliverable documentation content (CDRL) is too long.	0.5
65	Because of more than one contractor, the solution of the some problems can be time consuming.	0.5
66	Some collected process metrics are not evaluated, so project managers may not be informed about the performance of the processes.	0.3
67	Staff have not received enough training in some areas	0.7
68	Yearly holiday of the personnel may be overlapped, and some works may not be performed within a certain schedule.	0.3
69	New CM tool is applied, Problems may occur during usage	0.9
70	CM staff is not experienced, and CM tool is not used efficiently.	0.9
71	During choosing design solution out of alternatives, the owners of the unchosen alternatives may not trust on the chosen alternative and may show lack of cooperation.	0.3
72	Schedule is not planned for trainings, so deviation from schedule can occur.	0.5
73	The allocated time for development phase is not sufficient	0.9
74	Schedule is optimistic, "best case," rather than realistic, "expected case"	0.5
75	Excessive schedule pressure reduces productivity	0.5
76	Schedule is based on estimation but estimation is performed a bit subjective (depends on the performer) not based on historical data. So, schedule may not be the deserved schedule.	0.5
77	Staff in configuration management is not experienced, that may affect the success of the project.	0.7
78	Leaving of project personnel/Being late for inefficient performance of the project personnel	0.5
79	Leaving of project personnel during development phases	0.5
80	Adding personnel to a late project	0.3
81	Staffing may be not stable because of external factors like personal allocation to other projects, or personnel to leave the job	0.3
82	Some requirements may need more effort than estimated	0.5
83	Current availability leaves no time to correct potential defects found occurring aboard new product.	0.3

Table 7 Organization's Risks with Probability Estimates (cont'd)

84	Approval cycle for required documentation is long. This affects the performing of other work on time.	0.5
85	Work definitions that are not covered in contract may be performed	0.9
86	New user requirements that are not covered in the contract	0.5
87	The cases for adding/changing/deleting requirements are not defined in the contract. So, actions related with requirements may affect the success of project.	0.7
88	Customer does not understand technical aspects of the system well, so specifications may change any time after customer approval	0.7
89	Customer who care less for the process but is interested only in the final product. This may cause the problem in the customer related process	0.3
90	Insufficient training of end user	0.5
91	Change requests for document context from the customer	0.7
92	Requirements may be changed, added or deleted. That may affect the project's schedule and context	0.5
93	CDR meeting and necessary approval may be late	0.7
94	Data provided by customer according to contract, may be provided late	0.9
95	MFD hardware provided by customer according to contract, may be provided late	0.5
96	Prime Contractor may give design decisions after baselined design document. That may lead to loss of effort in organization	0.3
97	We are highly dependent to Prime Contractor for getting test tool, if test tool delays then schedule also delays	0.5
98	Preparation of Software Design Descriptions may delay and that's why, coding activities may be in difficulty	0.3
99	A need may occur for CBS licensing from Prime Contractor	0.3
100	Late comment from Prime Contractor for test documents, and change request for test documents during performing tests	0.5
101	Answer/approval time may be late because of conflicts between customer, users, and associated contractors.	0.7
102	Project may be cancelled by government because of its high budget, and conflicts between contractors	0.1

3.3.4 Risk Impact

Risk impact is the magnitude of financial loss resulting from risk's occurrence. In other words, negative impact a risk might have for the organization.

Impact value for each risk item is assigned subjectively by the organization. Impact for each risk item is assigned financially in the range of '1-10'. In this study, impact of each of the risk items on the project goals are assumed by the organization as low [1-3], medium[3-7], high[7-9] or very high[9-10].

According to these values, subjective impact estimates for the risk items are shown in Table 8.

Table 8 Organization's Risks with Impact Estimates

RISK NO	RISK ITEM	IMPACT
1	Requirements are changing and new requirements are added although requirement document is baselined. So, final delivery on time is getting harder because of changed and new requirements.	8
2	Requirements may not be defined on time and may be changed after the approval of requirements document	7
3	Customer introducing new system requirements without budget or schedule relief this is muddying the project's lines of authority	8
4	Incomplete requirements specification due to an uncertain customer	6
5	Current System Requirements are not well-defined, and some system requirements may be caught	8
6	There are some TBDs "To Be Determined" in requirement specification document. These TBDs should be determined before the release of requirement specification document.	7
7	Some requirements are not clear to fully understand, and may lead to wrong interpretation.	6
8	Development of extra software functions that are not required (gold-plating) extends the schedule	5
9	X module has been positioned wrongly in the project. There may be lack of system requirements for AVINT that is not included in the contract	7
10	Customer does not have a solid idea of what is required, and think to have unwritten requirements/expectations.	6
11	Requirements demand the use of new analysis, design or testing methods.	8

Table 8 Organization's Risks with Impact Estimates (cont'd)

12	Technology for this project is new to organization. Organization does not have sufficient knowledge in this area	5
13	Inappropriate design solution leads to redesign and reimplementation	4
14	Taking of risky design decisions in terms of project schedule and personnel number	4
15	Design solutions are not selected by objective evaluation, so it may be difficult to have solutions for all the requirements.	6
16	Developing the wrong user interface	4
17	Interdependency commitments might change without everyone being informed, and that might result in interface defects	5
18	System interface information may not be provided on time and that is why, product delivery may be late	4
19	Possibility of interface conflicts in the system design	6
20	Software builds with interface with vendor supplied software products that are unproven	3
21	Product will be used with hardware, but the interfaces of the software with the hardware are not well defined yet.	5
22	Size of Ada executable and slow execution may exceed hardware and timing limitations	2
23	Testers have not involved in analyzing requirements	4
24	RISC based hardware shall be used in the project. This technology is not well known by project the personnel. That is why, software development activities may be late	5
25	Because of tight schedule, sufficient unit testing is not performed	6
26	There is a lack of experienced C programmers, code may be inefficient/late	4
27	Design specifications are not in sufficient detail to write the code.	2
28	During the establishment of test environment, the selection of the configuration items with correct revisions is not checked, so risk for selecting wrong revisions for testing	3
29	The software ordered for testing the system may be delayed due to a "backorder" status resulting schedule change to a critical path activity	7
30	Just in time delivery of software will result in too-little time to integrate and field fix defects	5
31	There may be deviations from test results because of integration of unfinished CSCIs coming from Prime Contractor	6
32	There is only limited time for testing	5
33	All contractors are not part of the integration team	6
34	Integrated testing dependent upon multiple activity. Testing may fail	4

Table 8 Organization's Risks with Impact Estimates (cont'd)

35	Leaving of some works after acceptance tests due to reasons not from STM	3
36	High percentage of defects occurring in system acceptance tests/Risk of customer unsatisfaction	9
37	Planning some activities is nearly impossible because integration and acceptance process is not clear	4
38	Maintenance people are not involved early in the design, because maintenance planning is not performed before.	3
39	Design is not performed by considering maintenance expectations.	4
40	Organization has not implemented this level of security before.	2
41	The design related with human/user interfaces of the product may not be as what the user wants.	5
42	Project manager is undercut and new requirements are introduced: these may remain hidden and no test cases will be developed for them	4
43	The lack of standardized unit test descriptions and test methods in the organization	7
44	Inaccurate metrics may cause to wrong interpretation of process performances	3
45	Some written processes may not be followed	8
46	Development processes are not well measured to evaluate the meeting of productivity and quality goals.	4
47	Some new developers are not familiar with development processes and plans.	2
48	New requirements are added to the system but adequate analysis is not performed	6
49	We have never tried to make 10 computers work together like this; it could delay final system acceptance	5
50	Providing of Software Integration Environment by customer may not be performed	6
51	Some documentations coming from prime contractors are in different format than ours. Traceability may be difficult between documents in two different formats.	4
52	Technology to be built is new to the organization	5
53	Operation in an unfamiliar or unproved software environment causes unforeseen problems	5
54	Risk of video quality being low	7
55	Loss of data during conversation from one system to another	8
56	HA and VTE simulators are needed for more efficiency in the Software Development Activities. These simulators may not be provided	6
57	Needed CSCI versions may not be provided from Prime Contractor to use in software tests	7

Table 8 Organization's Risks with Impact Estimates (cont'd)

58	Estimation is not based on historical data	7
59	Preparation of related documents for Avionic Emulator that are covered in contract but not covered in Work Breakdown Structure	8
60	Planning is not based on experienced estimation process. So, no reliable effort estimate	7
61	People at all levels are not included in planning their own work	5
62	Customer is not willing to participate in reviews	5
63	No real cooperation between contractors	4
64	It takes too long to resolve issues with the customer. Customer approval of deliverable documentation content (CDRL) is too long.	5
65	Because of more than one contractor, the solution of the some problems can be time consuming.	4
66	Some collected process metrics are not evaluated, so project managers may not be informed about the performance of the processes.	3
67	Staff have not received enough training in some areas	6
68	Yearly holiday of the personnel may be overlapped, and some works may not be performed within a certain schedule.	2
69	New CM tool is applied, Problems may occur during usage	6
70	CM staff is not experienced, and CM tool is not used efficiently.	6
71	During choosing design solution out of alternatives, the owners of the unchosen alternatives may not trust on the chosen alternative and may show lack of cooperation.	3
72	Schedule is not planned for trainings, so deviation from schedule can occur.	4
73	The allocated time for development phase is not sufficient	6
74	Schedule is optimistic, "best case," rather than realistic, "expected case"	7
75	Excessive schedule pressure reduces productivity	6
76	Schedule is based on estimation but estimation is performed a bit subjective (depends on the performer) not based on historical data. So, schedule may not be the deserved schedule.	5
77	Staff in configuration management is not experienced, that may affect the success of the project.	6
78	Leaving of project personnel/Being late for inefficient performance of the project personnel	7
79	Leaving of project personnel during development phases	8
80	Adding personnel to a late project	4

Table 8 Organization's Risks with Impact Estimates (cont'd)

81	Staffing may be not stable because of external factors like personal allocation to other projects, or personnel to leave the job	7
82	Some requirements may need more effort than estimated	4
83	Current availability leaves no time to correct potential defects found occurring aboard new product.	5
84	Approval cycle for required documentation is long. This affects the performing of other work on time.	4
85	Work definitions that are not covered in contract may be performed	8
86	New user requirements that are not covered in the contract	7
87	The cases for adding/changing/deleting requirements are not defined in the contract. So, actions related with requirements may affect the success of project.	7
88	Customer does not understand technical aspects of the system well, so specifications may change any time after customer approval	6
89	Customer who care less for the process but is interested only in the final product. This may cause the problem in the customer related process	5
90	Insufficient training of end user	4
91	Change requests for document context from the customer	3
92	Requirements may be changed, added or deleted. That may affect the project's schedule and context	8
93	CDR meeting and necessary approval may be late	5
94	Data provided by customer according to contract, may be provided late	6
95	MFD hardware provided by customer according to contract, may be provided late	7
96	Prime Contractor may give design decisions after baselined design document. That may lead to loss of effort in organization	8
97	We are highly dependent to Prime Contractor for getting test tool, if test tool delays then schedule also delays	7
98	Preparation of Software Design Descriptions may delay and that's why, coding activities may be in difficulty	5
99	A need may occur for CBS licensing from Prime Contractor	6
100	Late comment from Prime Contractor for test documents, and change request for test documents during performing tests	6
101	Answer/approval time may be late because of conflicts between customer, users, and associated contractors.	8
102	Project may be cancelled by government because of its high budget, and conflicts.	10

3.3.5 Risk Exposure

Risk exposure is the overall threat of the eack risk item. Most organization use the method 1 to calculate risk exposure.

3.3.5.1 Method 1 (Qualitative)

Combination of risk probability and risk impact values to calculate risk exposure values. Range for exposure values are 'High', 'Medium' and 'Low'.

> High: Unacceptable. Major disruption is likely. Different approach required. Priority management decision required.
>
> Medium: Moderate. Some disruption. An alternate approach might be required. Additional management attention might be needed.
>
> Low: Low. Minimal impact. Minimal oversight required to ensure risk remains low.

Here, the limits for 'High', 'Medium' and 'Low' are management decisions. Table 9 is an example for the method 1.

Table 9 Risk Exposure Values for Method 1

Probability	*RISK EXPOSURE*									
0.9	*Low*	*Medium*	*Medium*	*Medium*	*High*	*High*	*High*	*High*	*High*	*High*
0.7	*Low*	*Medium*	*Medium*	*Medium*	*Medium*	*Medium*	*Medium*	*High*	*High*	*High*
0.5	*Low*	*Low*	*Low*	*Medium*	*Medium*	*Medium*	*Medium*	*High*	*High*	*High*
0.3	*Low*	*Low*	*Low*	*Low*	*Medium*	*Medium*	*Medium*	*Medium*	*High*	*High*
0.1	*Low*	*Low*	*Low*	*Low*	*Low*	*Medium*	*Medium*	*Medium*	*Medium*	*High*
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
	IMPACT									

These risk exposure values can be used in prioritization of risks, but cannot be directly used in quantifying risk management. For this reason, method 2 is offered.

3.3.5.2 Method 2 (Quantifying)

Risk exposure are calculated as product of probability and impact of a risk. **(**Risk Exposure = (Probability of the risk) ***** (Risk impact)**)**. Range for the exposure values are integer values between '1-10'. Table 10 is used if method 2 is chosen.

Table 10 Risk Exposure Values for Method 2

PROBABILITY	RISK EXPOSURE									
0.9	*0.9*	*1.8*	*2.7*	*3.6*	*4.5*	*5.4*	*6.3*	*7.2*	*8.1*	*9.0*
0.7	*0.7*	*1.4*	*2.1*	*2.8*	*3.5*	*4.2*	*4.9*	*5.6*	*6.3*	*7.0*
0.5	*0.5*	*1.0*	*1.5*	*2.0*	*2.5*	*3.0*	*3.5*	*4.0*	*4.5*	*5.0*
0.3	*0.3*	*0.6*	*0.9*	*1.2*	*1.5*	*1.8*	*2.1*	*2.4*	*2.7*	*3.0*
0.1	*0.1*	*0.2*	*0.3*	*0.4*	*0.5*	*0.6*	*0.7*	*0.8*	*0.9*	*1.0*
	1	2	3	4	5	6	7	8	9	10
	IMPACT									

Method 2 is used for the rest of the study, because these exposure values can be directly used in quantifying risk management.

According to Method 2, exposure values for the risk items are shown in Table 11.

Table 11 Organization's Risks with Exposure Estimates

RISK NO	RISK ITEM	EXPOSURE
1	Requirements are changing and new requirements are added although requirement document is baselined. So, final delivery on time is getting harder because of changed and new requirements.	5.6
2	Requirements may not be defined on time and may be changed after the approval of requirements document	3.5
3	Customer introducing new system requirements without budget or schedule relief this is muddying the project's lines of authority	2.4
4	Incomplete requirements specification due to an uncertain customer	3
5	Current System Requirements are not well-defined, and some system requirements may be caught	5.6
6	There are some TBDs "To Be Determined" in requirement specification document. These TBDs should be determined before the release of requirement specification document.	4.9
7	Some requirements are not clear to fully understand, and may lead to wrong interpretation.	1.8
8	Development of extra software functions that are not required (gold-plating) extends the schedule	0.5
9	X module has been positioned wrongly in the project. There may be lack of system requirements for AVINT that is not included in the contract	3.5
10	Customer does not have a solid idea of what is required, and think to have unwritten requirements/expectations.	4.2
11	Requirements demand the use of new analysis, design or testing methods.	2.4
12	Technology for this project is new to organization. Organization does not have sufficient knowledge in this area	1.5
13	Inappropriate design solution leads to redesign and reimplementation	2
14	Taking of risky design decisions in terms of project schedule and personnel number	2
15	Design solutions are not selected by objective evaluation, so it may be difficult to have solutions for all the requirements.	4.2
16	Developing the wrong user interface	1.2
17	Interdependency commitments might change without everyone being informed, and that might result in interface defects	0.5
18	System interface information may not be provided on time and that is why, product delivery may be late	1.2

Table 11 Organization's Risks with Exposure Estimates (cont'd)

19	Possibility of interface conflicts in the system design	3
20	Software builds with interface with vendor supplied software products that are unproven	1.5
21	Product will be used with hardware, but the interfaces of the software with the hardware are not well defined yet.	3.5
22	Size of Ada executable and slow execution may exceed hardware and timing limitations	0.6
23	Testers have not involved in analyzing requirements	2.8
24	RISC based hardware shall be used in the project. This technology is not well known by project the personnel. That is why, software development activities may be late	2.5
25	Because of tight schedule, sufficient unit testing is not performed	5.4
26	There is a lack of experienced C programmers, code may be inefficient/late	2
27	Design specifications are not in sufficient detail to write the code.	0.6
28	During the establishment of test environment, the selection of the configuration items with correct revisions is not checked, so risk for selecting wrong revisions for testing	0.9
29	The software ordered for testing the system may be delayed due to a "backorder" status resulting schedule change to a critical path activity	2.1
30	Just in time delivery of software will result in too-little time to integrate and field fix defects	1.5
31	There may be deviations from test results because of integration of unfinished CSCIs coming from Prime Contractor	3
32	There is only limited time for testing	3.5
33	All contractors are not part of the integration team	4.2
34	Integrated testing dependent upon multiple activity. Testing may fail	2
35	Leaving of some works after acceptance tests due to reasons not from STM	1.5
36	High percentage of defects occurring in system acceptance tests/Risk of customer unsatisfaction	4.5
37	Planning some activities is nearly impossible because integration and acceptance process is not clear	2.8
38	Maintenance people are not involved early in the design, because maintenance planning is not performed before.	2.1
39	Design is not performed by considering maintenance expectations.	2.8

Table 11 Organization's Risks with Exposure Estimates (cont'd)

40	Organization has not implemented this level of security before.	0.6
41	The design related with human/user interfaces of the product may not be as what the user wants.	1.5
42	Project manager is undercut and new requirements are introduced: these may remain hidden and no test cases will be developed for them	1.2
43	The lack of standardized unit test descriptions and test methods in the organization	3.5
44	Inaccurate metrics may cause to wrong interpretation of process performances	1.5
45	Some written processes may not be followed	2.4
46	Development processes are not well measured to evaluate the meeting of productivity and quality goals.	2
47	Some new developers are not familiar with development processes and plans.	1.4
48	New requirements are added to the system but adequate analysis is not performed	3
49	We have never tried to make 10 computers work together like this; it could delay final system acceptance	3.5
50	Providing of Software Integration Environment by customer may not be performed	1.8
51	Some documentations coming from prime contractors are in different format than ours. Traceability may be difficult between documents in two different formats.	1.2
52	Technology to be built is new to the organization	1.5
53	Operation in an unfamiliar or unproved software environment causes problems	3.5
54	Risk of video quality being low	3.5
55	Loss of data during conversation from one system to another	2.4
56	HA and VTE simulators are needed for more efficiency in the Software Development Activities. These simulators may not be provided	3
57	Needed CSCI versions may not be provided from Prime Contractor to use in software tests	3.5
58	Estimation is not based on historical data	4.9
59	Preparation of related documents for Avionic Emulator that are covered in contract but not covered in Work Breakdown Structure	7.2
60	Planning is not based on experienced estimation process. So, no reliable effort estimate	4.9
61	People at all levels are not included in planning their own work	2.5
62	Customer is not willing to participate in reviews	3.5
63	No real cooperation between contractors	2.8

Table 11 Organization's Risks with Exposure Estimates (cont'd)

64	It takes too long to resolve issues with the customer. Customer approval of deliverable documentation content (CDRL) is too long.	2.5
65	Because of more than one contractor, the solution of the some problems can be time consuming.	2
66	Some collected process metrics are not evaluated, so project managers may not be informed about the performance of the processes.	0.9
67	Staff have not received enough training in some areas	4.2
68	Yearly holiday of the personnel may be overlapped, and some works may not be performed within a certain schedule.	0.6
69	New CM tool is applied, Problems may occur during usage	5.4
70	CM staff is not experienced, and CM tool is not used efficiently.	5.4
71	During choosing design solution out of alternatives, the owners of the unchosen alternatives may not trust on the chosen alternative and may show lack of cooperation.	0.9
72	Schedule is not planned for trainings, so deviation from schedule can occur.	2
73	The allocated time for development phase is not sufficient	5.4
74	Schedule is optimistic, "best case," rather than realistic, "expected case"	3.5
75	Excessive schedule pressure reduces productivity	3
76	Schedule is based on estimation but estimation is performed a bit subjective (depends on the performer) not based on historical data. So, schedule may not be the deserved schedule.	2.5
77	Staff in configuration management is not experienced, that may affect the success of the project.	4.2
78	Leaving of project personnel/Being late for inefficient performance of the project personnel	3.5
79	Leaving of project personnel during development phases	4
80	Adding personnel to a late project	1.2
81	Staffing may be not stable because of external factors like personal allocation to other projects, or personnel to leave the job	2.1
82	Some requirements may need more effort than estimated	2
83	Current availability leaves no time to correct potential defects found occurring aboard new product.	1.5
84	Approval cycle for required documentation is long. This affects the performing of other work on time.	2

Table 11 Organization's Risks with Exposure Estimates (cont'd)

85	Work definitions that are not covered in contract may be performed	7.2
86	New user requirements that are not covered in the contract	3.5
87	The cases for adding/changing/deleting requirements are not defined in the contract. So, actions related with requirements may affect the success of project.	4.9
88	Customer does not understand technical aspects of the system well, so specifications may change any time after customer approval	4.2
89	Customer who care less for the process but is interested only in the final product. This may cause the problem in the customer related process	1.5
90	Insufficient training of end user	2
91	Change requests for document context from the customer	2.1
92	Requirements may be changed, added or deleted. That may affect the project's schedule and context	4
93	CDR meeting and necessary approval may be late	3.5
94	Data provided by customer according to contract, may be provided late	5.4
95	MFD hardware provided by customer according to contract, may be provided late	3.5
96	Prime Contractor may give design decisions after baselined design document. That may lead to loss of effort in organization	2.4
97	We are highly dependent to Prime Contractor for getting test tool, if test tool delays then schedule also delays	3.5
98	Preparation of Software Design Descriptions may delay and that's why, coding activities may be in difficulty	1.5
99	A need may occur for CBS licensing from Prime Contractor	1.8
100	Late comment from Prime Contractor for test documents, and change request for test documents during performing tests	3
101	Answer/approval time may be late because of conflicts between customer, users, and associated contractors.	5.6
102	Project may be cancelled by government because of its high budget, and conflicts between contractors	1

3.4. Risk Control

3.4.1 Risk Mitigation Action

Once the risks have been identified, risk mitigation actions are planned. Risk mitigation actions, based on the project specific factors, are developed and implemented to proactively reduce the potential exposure of risk occurrence, and so to reduce impacts on achieving objectives.

Risk mitigation actions can be either precautionary actions or emergency actions. Risk mitigation actions target the followings:

- Reduce and probability that the risk will actually turn into a problem
- Reduce the impact of the risk
- Shift the time frame for beginning of the risk occurrence
- Eliminate the present circumstances that give rise to the risk

In the light of this definition, risk mitigation actions for risk items are described in Table 12.

Table 12 Organization's Risks with Risk Mitigation Actions

RISK NO	RISK ITEM	RISK MITIGATION ACTION
1	Requirements are changing and new requirements are added although requirement document is baselined. So, final delivery on time is getting harder because of changed and new requirements.	Customer shall be convinced that changes in requirements will have an impact on schedule, negotiation shall be performed with customer
2	Requirements may not be defined on time and may be changed after the approval of requirements document	Prestudy shall be performed in order to provide all requirements to be determined in SRS phase, and coordination shall be established with prime contractors to prevent the change of the requirements
3	Customer introducing new system requirements without budget or schedule relief this is muddying the project's lines of authority	This needs the revision of contract. Contract department shall perform a study to cover this scenario and present it to the customer.

Table 12 Organization's Risks with Risk Mitigation Actions (cont'd)

4	Incomplete requirements specification due to an uncertain customer	Prestudy shall be performed in order to determine all incomplete requirements before releasing of requirement specification document. Prototype shall be build and shown to the customer to help in determination
5	Current System Requirements are not well-defined, and some system requirements may be caught	Effective requirement analysis shall be performed, and experienced personnel shall be gathered for this analysis
6	There are some TBDs "To Be Determined" in requirement specification document. These TBDs should be determined before the release of requirement specification document.	Prestudy shall be performed in order to determine all TBDs before releasing of requirement specification document. Prototype shall be built and shown to the customer to help in determination
7	Some requirements are not clear to fully understand, and may lead to wrong interpretation.	Develop a prototype/get the requirements reviewed by the client
8	Development of extra software functions that are not required (gold-plating) extends the schedule	Personnel shall be oriented just to focus on requirements in order to prevent from gold-plating
9	X module has been positioned wrongly in the project. There may be lack of system requirements for AVINT that is not included in the contract	A formal meeting shall be arranged and gathered with the customer for AVINT requirements
10	Customer does not have a solid idea of what is required, and think to have unwritten requirements/expectations.	Prototype shall be built and shown to the customer to help for unwritten requirements/expectations
11	Requirements demand the use of new analysis, design or testing methods.	Experienced personnel on this subject shall be employed
12	Technology for this project is new to organization. Organization does not have sufficient knowledge in this area	Some literature study shall be performed about this technology
13	Inappropriate design solution leads to redesign and reimplementation	DAR (Decision Analysis & Resolution) procedure shall be written for choosing one of the design alternatives
14	Taking of risky design decisions in terms of project schedule and personnel number	Design decisions shall be taken by considering project schedule and available personnel
15	Design solutions are not selected by objective evaluation, so it may be difficult to have solutions for all the requirements.	DAR (Decision Analysis & Resolution) procedure shall be written for choosing one of the design alternatives
16	Developing the wrong user interface	The concept of IDD (Interface Design Descriptions) shall be covered in SDD (Software Design Description) document

Table 12 Organization's Risks with Risk Mitigation Actions (cont'd)

17	Interdependency commitments might change without everyone being informed, and that might result in interface defects	Changed interdependency commitments shall be mentioned in project's weekly status meetings for everyone being informed
18	System interface information may not be provided on time and that is why, product delivery may be late	Necessary actions shall be taken about contract items of system interface information
19	Possibility of interface conflicts in the system design	ICD document shall be prepared to prevent the possibility of interface conflicts in the system design
20	Software builds with interface with vendor supplied software products that are unproven	Acceptance control tests shall be performed for the vendor supplied software products
21	Product will be used with hardware, but the interfaces of the software with the hardware are not well defined yet.	Interface Design Description document shall be produced to show the interfaces of the software with the hardware
22	Size of Ada executable and slow execution may exceed hardware and timing limitations	Timing limitations shall be tested, a new solution shall be searched if problem occurs in the test
23	Testers have not involved in analyzing requirements	Sufficient time shall be given to testers to read and understand system/software requirements
24	RISC based hardware shall be used in the project. This technology is not well known by project the personnel. That is why, software development activities may be late	Prestudy shall be performed by the personnel on RISC based hardware by obtaining the related hardware before system design phase
25	Because of tight schedule, sufficient unit testing is not performed	CSCI tests shall be performed more strictly
26	There is a lack of experienced C programmers, code may be inefficient/late	Code review shall be performed in much more detail
27	Design specifications are not in sufficient detail to write the code.	Design specifications shall be re-written clearly in order to write the sufficient detailed code
28	During the establishment of test environment, the selection of the configuration items with correct revisions is not checked, so risk for selecting wrong revisions for testing	The selection of configuration items shall be performed in the coordination of CM Specialist
29	The software ordered for testing the system may be delayed due to a "backorder" status resulting schedule change to a critical path activity	A coordination shall be performed with the supplier in order to get the software as soon as possible
30	Just in time delivery of software will result in too-little time to integrate and field fix defects	Integration test shall be performed in full details. Detected defects shall be fixed

Table 12 Organization's Risks with Risk Mitigation Actions (cont'd)

31	There may be deviations from test results because of integration of unfinished CSCIs coming from Prime Contractor	Coordination shall be performed with Prime Contractor that integration activities of critical CSCIs in test scenarios to be done faster and Stub codes to continue to be used at other CSCIs
32	There is only limited time for testing	Increase code inspection
33	All contractors are not part of the integration team	A meeting shall be performed by the participation of all contractors, the coordination shall be decided in this meeting
34	Integrated testing dependent upon multiple activity. Testing may fail	The tasks of the every activity shall be written and tested in integration test cases.
35	Leaving of some works after acceptance tests due to reasons not from STM	Customer/User shall be convinced that acceptance of the project shall be done on time and at one time
36	High percentage of defects occurring in system acceptance tests/Risk of customer unsatisfaction	The study of detailed ICD shall be performed to prevent unsatisfaction and the problems in the phases of System Integration and Testing
37	Planning some activities is nearly impossible because integration and acceptance process is not clear	Planning shall be performed by coordinating with Prime Contractors
38	Maintenance people are not involved early in the design, because maintenance planning is not performed before.	If maintenance contract is signed, design shall be improved to cover maintenance requirements
39	Design is not performed by considering maintenance expectations.	If maintenance contract is signed, design shall be improved to cover maintenance requirements
40	Organization has not implemented this level of security before.	Security controls shall be performed by QA Specialist periodically
41	The design related with human/user interfaces of the product may not be as what the user wants.	Design related with human/user interfaces shall be presented to the customer in a meeting
42	Project manager is undercut and new requirements are introduced: these may remain hidden and no test cases will be developed for them	New requirements are introduced to the project means the update of SSS and SRS. Software Test Descriptions shall be updated (new test cases shall be written for new requirements) to trace every requirement with any test cases.
43	The lack of standardized unit test descriptions and test methods in the organization	Organization's procedures shall be written by the responsible personnel
44	Inaccurate metrics may cause to wrong interpretation of process performances	New metrics for the critical processes shall be defined and followed

Table 12 Organization's Risks with Risk Mitigation Actions (cont'd)

45	Some written processes may not be followed	Quality Assurance audits shall be performed on certain processes, and processes shall be provided to be followed
46	Development processes are not well measured to evaluate the meeting of productivity and quality goals.	New metrics for development processes shall be defined, and followed to evaluate the meeting of productivity and quality goals
47	Some new developers are not familiar with development processes and plans.	These new developers shall be given orientation from the organization about the development processes and plans
48	New requirements are added to the system but adequate analysis is not performed	System requirement analysis shall be performed for new requirements
49	We have never tried to make 10 computers work together like this; it could delay final system acceptance	Before final system acceptance test, this scenario shall be tested in the test environment
50	Providing of Software Integration Environment by customer may not be performed	Coordination shall be performed with the customer for getting the environment on time
51	Some documentations coming from prime contractors are in different format than ours. Traceability may be difficult between documents in two different formats.	Traceability matrixes shall be prepared between customer documents and our documents.
52	Technology to be built is new to the organization	Some literature study shall be performed about this technology
53	Operation in an unfamiliar or unproved software environment causes unforeseen problems	Some literature study shall be performed about this software environment
54	Risk of video quality being low	RS 170 video quality shall be tested and shown to the customer
55	Loss of data during conversation from one system to another	Data of the system shall be backed up before conversation
56	HA and VTE simulators are needed for more efficiency in the Software Development Activities. These simulators may not be provided	Coordination shall be performed with the customer for getting the simulators on time
57	Needed CSCI versions may not be provided from Prime Contractor to use in software tests	Coordination shall be performed with the customer for getting the needed CSCI versions on time
58	Estimation is not based on historical data	The schedule, budget and effort of the project shall be reviewed in terms of the old projects' data

Table 12 Organization's Risks with Risk Mitigation Actions (cont'd)

59	Preparation of related documents for Avionic Emulator that are covered in contract but not covered in Work Breakdown Structure	New work force shall be added for documentation
60	Planning is not based on experienced estimation process. So, no reliable effort estimate	Planning shall be re-done by considering old projects' plan vs actual data
61	People at all levels are not included in planning their own work	The plan makers shall consider the task assignments of the personnel during planning of the people
62	Customer is not willing to participate in reviews	Customer shall be convinced to participate in reviews, and follow the project progress
63	No real cooperation between contractors	A meeting shall be performed by the participation of all contractors, the coordination shall be decided in this meeting
64	It takes too long to resolve issues with the customer. Customer approval of deliverable documentation content (CDRL) is too long.	Customer shall be convinced that if the approval of the document is longer than schedule, then project schedule will be longer
65	Because of more than one contractor, the solution of the some problems can be time consuming.	A meeting shall be performed by the participation of all contractors, the coordination shall be decided in this meeting
66	Some collected process metrics are not evaluated, so project managers may not be informed about the performance of the processes.	Project managers shall define project specific metrics, and follow these metrics along the project.
67	Staff have not received enough training in some areas	Staff shall receive enough internal training in some areas
68	Yearly holiday of the personnel may be overlapped, and some works may not be performed within a certain schedule.	Personnel holiday plan shall be prepared in a way that works will finish on time
69	New CM tool is applied, Problems may occur during usage	Training for this CM tool shall be taken by CM Specialist
70	CM staff is not experienced, and CM tool is not used efficiently.	Training for CM concepts and CM tool shall be taken by CM Specialist
71	During choosing design solution out of alternatives, the owners of the unchosen alternatives may not trust on the chosen alternative and may show lack of cooperation.	DAR (Decision Analysis & Resolution) procedure shall be written for choosing one of the design alternatives
72	Schedule is not planned for trainings, so deviation from schedule can occur.	Project plan and schedule shall be updated in the way that covering trainings

Table 12 Organization’s Risks with Risk Mitigation Actions (cont’d)

73	The allocated time for development phase is not sufficient	Work plan over the standard working time shall be planned and implemented
74	Schedule is optimistic, "best case," rather than realistic, "expected case"	Negotiation shall be performed for better schedule with the customer, and negotiation shall be performed for resources with the upper management
75	Excessive schedule pressure reduces productivity	Negotiation shall be performed for better schedule with the customer, and negotiation shall be performed for resources with the upper management
76	Schedule is based on estimation but estimation is performed a bit subjective (depends on the performer) not based on historical data. So, schedule may not be the deserved schedule.	The schedule of the project shall be reviewed in terms of the old projects' data, and shall be updated if necessary.
77	Staff in configuration management is not experienced, that may affect the success of the project.	Training for CM concepts shall be taken by CM Specialist
78	Leaving of project personnel/Being late for inefficient performance of the project personnel	The expectations of the personnel shall be met without creating risks
79	Leaving of project personnel during development phases	The expectations of the personnel shall be met without creating risks
80	Adding personnel to a late project	Orientation about project status shall be given to added personnel
81	Staffing may be not stable because of external factors like personal allocation to other projects, or personnel to leave the job	The expectations of the personnel shall be met without creating risks
82	Some requirements may need more effort than estimated	The design, needing minimum work effort, shall be chosen.
83	Current availability leaves no time to correct potential defects found occurring aboard new product.	Tests shall be performed with full coverage, and detected defects shall be corrected until the software passes the tests
84	Approval cycle for required documentation is long. This affects the performing of other work on time.	Customer shall be convinced that if the approval of the document is longer than schedule, then project schedule will be longer
85	Work definitions that are not covered in contract may be performed	Addition effort shall be planned and given
86	New user requirements that are not covered in the contract	The requirements shall be minimized by the negotiations

Table 12 Organization's Risks with Risk Mitigation Actions (cont'd)

87	The cases for adding/changing/deleting requirements are not defined in the contract. So, actions related with requirements may affect the success of project.	Contract shall be updated in a way that including the cases for adding/changing/deleting requirements
88	Customer does not understand technical aspects of the system well, so specifications may change any time after customer approval	At the milestone meetings (at the end of system requirement, system design, software requirement, software design and testing phase), the properties/capabilities of the system shall be explained to the customer
89	Customer who care less for the process but is interested only in the final product. This may cause the problem in the customer related process	Customer shall be encouraged to perform their responsibilities in the customer related process
90	Insufficient training of end user	End users shall be trained by our organization
91	Change requests for document context from the customer	Coordination shall be performed with the customer for taking necessary preventive actions on this subject
92	Requirements may be changed, added or deleted. That may affect the project's schedule and context	Project schedule and context shall be updated and presented to the customer for the approval
93	CDR meeting and necessary approval may be late	Coordination shall be performed with the customer for CDR meeting and necessary approval made on time
94	Data provided by customer according to contract, may be provided late	Coordination shall be performed with the customer for getting the data on time
95	MFD hardware provided by customer according to contract, may be provided late	Coordination shall be performed with the customer for getting the MFD hardware on time
96	Prime Contractor may give design decisions after baselined design document. That may lead to loss of effort in organization	Prime Contractor shall be reminded that design decisions should be given before baselined design document
97	We are highly dependent to Prime Contractor for getting test tool, if test tool delays then schedule also delays	Coordination shall be performed with the Prime Contractor for getting the test tool on time
98	Preparation of Software Design Descriptions may delay and that's why, coding activities may be in difficulty	Coordination shall be performed with the Prime Contractor in order to prevent SDD document being delivered late

Table 12 Organization's Risks with Risk Mitigation Actions (cont'd)

99	A need may occur for CBS licensing from Prime Contractor	Prestudy shall be performed about the necessity of CBS licensing. If necessary, Coordination shall be performed with the Prime Contractor for getting the CBS licensing on time
100	Late comment from Prime Contractor for test documents, and change request for test documents during performing tests	Coordination shall be performed with the Prime Contractor for getting comment and change requests (if exist) on time
101	Answer/approval time may be late because of conflicts between customer, users, and associated contractors.	The contacts shall be performed on a certain Prime Contractor
102	Project may be cancelled by government because of its high budget, and conflicts between contractors	In the suitable platforms, it is said that the project is the first national system in its area

3.4.2 Risk Mitigation Cost

Each risk mitigation action has a cost. In this study, man-hour and YTL (New Turkish Lira) are used as unit of cost. There are two different units of cost (man-hour and YTL) for the risk mitigation costs. YTL unit has been converted to man-hour unit by assuming "1 man-hour = 15 YTL".

In risk identification section (Section 3.3.1), a certain concern is mentioned. That is about identified risk items being orthogonal. Therefore, overestimation of risk mitigation costs are prevented by following the attention.

Resulting risk mitigation costs (consisting of preparation and execution costs) estimates for risk mitigation actions are shown in Table 13.

Table 13 Organization's Risks with Risk Mitigation Costs

RISK NO	RISK MITIGATION ACTION	RISK MITIGATION COST
1	Customer shall be convinced that changes in requirements will have an impact on schedule, negotiation shall be performed with customer	16 man-hour
2	Prestudy shall be performed in order to provide all requirements to be determined in SRS phase, and coordination shall be established with prime contractors to prevent the change of the requirements	120 man-hour
3	This needs the revision of contract. Contract department shall perform a study to cover this scenario and present it to the customer.	32 man-hour
4	Prestudy shall be performed in order to determine all incomplete requirements before releasing of requirement specification document. Prototype shall be build and shown to the customer to help in determination	160 man-hour
5	Effective requirement analysis shall be performed, and experienced personnel shall be gathered for this analysis	144 man-hour
6	Prestudy shall be performed in order to determine all TBDs before releasing of requirement specification document. Prototype shall be built and shown to the customer to help in determination	160 man-hour
7	Develop a prototype/get the requirements reviewed by the client	80 man-hour
8	Personnel shall be oriented just to focus on requirements in order to prevent from gold-plating	12 man-hour
9	A formal meeting shall be arranged and gathered with the customer for AVINT requirements	48 man-hour
10	Prototype shall be built and shown to the customer to help for unwritten requirements/expectations	80 man-hour
11	Experienced personnel on this subject shall be employed	3000 YTL
12	Some literature study shall be performed about this technology	64 man-hour
13	DAR (Decision Analysis & Resolution) procedure shall be written for choosing one of the design alternatives	40 man-hour
14	Design decisions shall be taken by considering project schedule and available personnel	24 man-hour
15	DAR (Decision Analysis & Resolution) procedure shall be written for choosing one of the design alternatives	40 man-hour
16	The concept of IDD (Interface Design Descriptions) shall be covered in SDD (Software Design Description) document	96 man-hour

Table 13 Organization's Risks with Risk Mitigation Costs (cont'd)

17	Changed interdependency commitments shall be mentioned in project's weekly status meetings for everyone being informed	20 man-hour
18	Necessary actions shall be taken about contract items of system interface information	32 man-hour
19	ICD document shall be prepared to prevent the possibility of interface conflicts in the system design	120 man-hour
20	Acceptance control tests shall be performed for the vendor supplied software products	72 man-hour
21	Interface Design Description document shall be produced to show the interfaces of the software with the hardware	96 man-hour
22	Timing limitations shall be tested, a new solution shall be searched if problem occurs in the test	72 man-hour
23	Sufficient time shall be given to testers to read and understand system/software requirements	80 man-hour
24	Prestudy shall be performed by the personnel on RISC based hardware by obtaining the related hardware before system design phase	64 man-hour
25	CSCI tests shall be performed more strictly	64 man-hour
26	Code review shall be performed in much more detail	48 man-hour
27	Design specifications shall be re-written clearly in order to write the sufficient detailed code	32 man-hour
28	The selection of configuration items shall be performed in the coordination of CM Specialist	16 man-hour
29	A coordination shall be performed with the supplier in order to get the software as soon as possible	8 man-hour
30	Integration test shall be performed in full details. Detected defects shall be fixed	64 man-hour
31	Coordination shall be performed with Prime Contractor that integration activities of critical CSCIs in test scenarios to be done faster and Stub codes to continue to be used at other CSCIs	16 man-hour
32	Increase code inspection	48 man-hour
33	A meeting shall be performed by the participation of all contractors, the coordination shall be decided in this meeting	40 man-hour
34	The tasks of the every activity shall be written and tested in integration test cases.	64 man-hour
35	Customer/User shall be convinced that acceptance of the project shall be done on time and at one time	16 man-hour

Table 13 Organization's Risks with Risk Mitigation Costs (cont'd)

36	The study of detailed ICD shall be performed to prevent unsatisfaction and the problems in the phases of System Integration and Testing	120 man-hour
37	Planning shall be performed by coordinating with Prime Contractors	16 man-hour
38	If maintenance contract is signed, design shall be improved to cover maintenance requirements	80 man-hour
39	If maintenance contract is signed, design shall be improved to cover maintenance requirements	80 man-hour
40	Security controls shall be performed by QA Specialist periodically	16 man-hour
41	Design related with human/user interfaces shall be presented to the customer in a meeting	32 man-hour
42	New requirements are introduced to the project means the update of SSS and SRS. Software Test Descriptions shall be updated (new test cases shall be written for new requirements) to trace every requirement with any test cases.	72 man-hour
43	Organization's procedures shall be written by the responsible personnel	112 man-hour
44	New metrics for the critical processes shall be defined and followed	32 man-hour
45	Quality Assurance audits shall be performed on certain processes, and processes shall be provided to be followed	40 man-hour
46	New metrics for development processes shall be defined, and followed to evaluate the meeting of productivity and quality goals	32 man-hour
47	These new developers shall be given orientation from the organization about the development processes and plans	40 man-hour
48	System requirement analysis shall be performed for new requirements	96 man-hour
49	Before final system acceptance test, this scenario shall be tested in the test environment	16 man-hour
50	Coordination shall be performed with the customer for getting the environment on time	16 man-hour
51	Traceability matrixes shall be prepared between customer documents and our documents.	28 man-hour
52	Some literature study shall be performed about this technology	64 man-hour
53	Some literature study shall be performed about this software environment	64 man-hour
54	RS 170 video quality shall be tested and shown to the customer	48 man-hour
55	Data of the system shall be backed up before conversation	8 man-hour
56	Coordination shall be performed with the customer for getting the simulators on time	16 man-hour

Table 13 Organization's Risks with Risk Mitigation Costs (cont'd)

57	Coordination shall be performed with the customer for getting the needed CSCI versions on time	16 man-hour
58	The schedule, budget and effort of the project shall be reviewed in terms of the old projects' data	40 man-hour
59	New work force shall be added for documentation	136 man-hour
60	Planning shall be re-done by considering old projects' plan vs actual data	40 man-hour
61	The plan makers shall consider the task assignments of the personnel during planning of the people	32 man-hour
62	Customer shall be convinced to participate in reviews, and follow the progress	16 man-hour
63	A meeting shall be performed by the participation of all contractors, the coordination shall be decided in this meeting	40 man-hour
64	Customer shall be convinced that if the approval of the document is longer than schedule, then project schedule will be longer	16 man-hour
65	A meeting shall be performed by the participation of all contractors, the coordination shall be decided in this meeting	40 man-hour
66	Project managers shall define project specific metrics, and follow these metrics along the project.	32 man-hour
67	Staff shall receive enough internal training in some areas	112 man hour
68	Personnel holiday plan shall be prepared in a way that works will finish on time	8 man-hour
69	Training for this CM tool shall be taken by CM Specialist	300 YTL
70	Training for CM concepts and CM tool shall be taken by CM Specialist	400 YTL
71	DAR (Decision Analysis & Resolution) procedure shall be written for choosing one of the design alternatives	40 man-hour
72	Project plan and schedule shall be updated in the way that covering trainings	16 man-hour
73	Work plan over the standard working time shall be planned and implemented	12 man-hour
74	Negotiation shall be performed for better schedule with the customer, and negotiation shall be performed for resources with the upper management	24 man-hour
75	Negotiation shall be performed for better schedule with the customer, and negotiation shall be performed for resources with the upper management	24 man-hour
76	The schedule of the project shall be reviewed in terms of the old projects' data, and shall be updated if necessary.	40 man-hour
77	Training for CM concepts shall be taken by CM Specialist	300 YTL
78	The expectations of the personnel shall be met without creating risks	72 man-hour + 2000 YTL

Table 13 Organization's Risks with Risk Mitigation Costs (cont'd)

79	The expectations of the personnel shall be met without creating risks	72 man-hour + 2000 YTL
80	Orientation about project status shall be given to added personnel	24 man-hour
81	The expectations of the personnel shall be met without creating risks	72 man-hour + 2000 YTL
82	The design, needing minimum work effort, shall be chosen.	8 man-hour
83	Tests shall be performed with full coverage, and detected defects shall be corrected until the software passes the tests	72 man-hour
84	Customer shall be convinced that if the approval of the document is longer than schedule, then project schedule will be longer	16 man-hour
85	Addition effort shall be planned and given	160 man-hour
86	The requirements shall be minimized by the negotiations	32 man-hour
87	Contract shall be updated in a way that including the cases for adding/changing/deleting requirements	48 man-hour
88	At the milestone meetings (at the end of system requirement, system design, software requirement, software design and testing phase), the properties/capabilities of the system shall be explained to the customer	72 man-hour
89	Customer shall be encouraged to perform their responsibilities in the customer related process	12 man-hour
90	End users shall be trained by our organization	40 man-hour
91	Coordination shall be performed with the customer for taking necessary preventive actions on this subject	16 man-hour
92	Project schedule and context shall be updated and presented to the customer for the approval	24 man-hour
93	Coordination shall be performed with the customer for CDR meeting and necessary approval made on time	16 man-hour
94	Coordination shall be performed with the customer for getting the data on time	16 man-hour
95	Coordination shall be performed with the customer for getting the MFD hardware on time	16 man-hour
96	Prime Contractor shall be reminded that design decisions should be given before baselined design document	16 man-hour
97	Coordination shall be performed with the Prime Contractor for getting the test tool on time	16 man-hour
98	Coordination shall be performed with the Prime Contractor in order to prevent SDD document being delivered late	16 man-hour

Table 13 Organization's Risks with Risk Mitigation Costs (cont'd)

99	Prestudy shall be performed about the necessity of CBS licensing. If necessary, Coordination shall be performed with the Prime Contractor for getting the CBS licensing on time	24 man-hour
100	Coordination shall be performed with the Prime Contractor for getting comment and change requests (if exist) on time	16 man-hour
101	The contacts shall be performed on a certain Prime Contractor	32 man-hour
102	In the suitable platforms, it is said that the project is the first national system in its area	20 man-hour

3.4.3 Probability for Mitigation

There is no guarantee that risk mitigation action prevent/reduce risk occurrence/exposure. For each risk item, there is probability that risk mitigation action prevent/reduce risk occurrence/exposure. The defined set of these probabilities determined by the organization is [0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9].

According to the values in this set, assigned subjective 'probability for mitigation' estimates for the risk items by the organization are shown in Table 14.

Table 14 Organization's Risk Mitigation Actions with Probability for Mitigation Values

RISK NO	RISK MITIGATION ACTION	Prob. for Mitigation
1	Customer shall be convinced that changes in requirements will have an impact on schedule, negotiation shall be performed with customer	0.5
2	Prestudy shall be performed in order to provide all requirements to be determined in SRS phase, and coordination shall be established with prime contractors to prevent the change of the requirements	0.6
3	This needs the revision of contract. Contract department shall perform a study to cover this scenario and present it to the customer.	0.7

Table 14 Organization's Risk Mitigation Actions with Probability for Mitigation Values (cont'd)

4	Prestudy shall be performed in order to determine all incomplete requirements before releasing of requirement specification document. Prototype shall be build and shown to the customer to help in determination	0.8
5	Effective requirement analysis shall be performed, and experienced personnel shall be gathered for this analysis	0.7
6	Prestudy shall be performed in order to determine all TBDs before releasing of requirement specification document. Prototype shall be built and shown to the customer to help in determination	0.8
7	Develop a prototype/get the requirements reviewed by the client	0.8
8	Personnel shall be oriented just to focus on requirements in order to prevent from gold-plating	0.9
9	A formal meeting shall be arranged and gathered with the customer for AVINT requirements	0.7
10	Prototype shall be built and shown to the customer to help for unwritten requirements/expectations	0.8
11	Experienced personnel on this subject shall be employed	0.8
12	Some literature study shall be performed about this technology	0.6
13	DAR (Decision Analysis & Resolution) procedure shall be written for choosing one of the design alternatives	0.9
14	Design decisions shall be taken by considering project schedule and available personnel	0.6
15	DAR (Decision Analysis & Resolution) procedure shall be written for choosing one of the design alternatives	0.9
16	The concept of IDD (Interface Design Descriptions) shall be covered in SDD (Software Design Description) document	0.8
17	Changed interdependency commitments shall be mentioned in project's weekly status meetings for everyone being informed	0.9
18	Necessary actions shall be taken about contract items of system interface information	0,7
19	ICD document shall be prepared to prevent the possibility of interface conflicts in the system design	0.8
20	Acceptance control tests shall be performed for the vendor supplied software products	0.9
21	Interface Design Description document shall be produced to show the interfaces of the software with the hardware	0.8

Table 14 Organization's Risk Mitigation Actions with Probability for Mitigation Values (cont'd)

22	Timing limitations shall be tested, a new solution shall be searched if problem occurs in the test	0.6
23	Sufficient time shall be given to testers to read and understand system/software requirements	0.7
24	Prestudy shall be performed by the personnel on RISC based hardware by obtaining the related hardware before system design phase	0.6
25	CSCI tests shall be performed more strictly	0.7
26	Code review shall be performed in much more detail	0.6
27	Design specifications shall be re-written clearly in order to write the sufficient detailed code	0.8
28	The selection of configuration items shall be performed in the coordination of CM Specialist	0.9
29	A coordination shall be performed with the supplier in order to get the software as soon as possible	0.3
30	Integration test shall be performed in full details. Detected defects shall be fixed	0.7
31	Coordination shall be performed with Prime Contractor that integration activities of critical CSCIs in test scenarios to be done faster and Stub codes to continue to be used at other CSCIs	0.5
32	Increase code inspection	0.6
33	A meeting shall be performed by the participation of all contractors, the coordination shall be decided in this meeting	0.7
34	The tasks of the every activity shall be written and tested in integration test cases.	0.7
35	Customer/User shall be convinced that acceptance of the project shall be done on time and at one time	0.5
36	The study of detailed ICD shall be performed to prevent unsatisfaction and the problems in the phases of System Integration and Testing	0.8
37	Planning shall be performed by coordinating with Prime Contractors	0.5
38	If maintenance contract is signed, design shall be improved to cover maintenance requirements	0.7
39	If maintenance contract is signed, design shall be improved to cover maintenance requirements	0.7
40	Security controls shall be performed by QA Specialist periodically	0.8
41	Design related with human/user interfaces shall be presented to the customer in a meeting	0.9

Table 14 Organization's Risk Mitigation Actions with Probability for Mitigation Values (cont'd)

42	New requirements are introduced to the project means the update of SSS and SRS. Software Test Descriptions shall be updated (new test cases shall be written for new requirements) to trace every requirement with any test cases.	0.8
43	Organization's procedures shall be written by the responsible personnel	0.9
44	New metrics for the critical processes shall be defined and followed	0.8
45	Quality Assurance audits shall be performed on certain processes, and processes shall be provided to be followed	0.9
46	New metrics for development processes shall be defined, and followed to evaluate the meeting of productivity and quality goals	0.8
47	These new developers shall be given orientation from the organization about the development processes and plans	0.9
48	System requirement analysis shall be performed for new requirements	0.8
49	Before final system acceptance test, this scenario shall be tested in the test environment	0.6
50	Coordination shall be performed with the customer for getting the environment on time	0.5
51	Traceability matrixes shall be prepared between customer documents and our documents.	0.9
52	Some literature study shall be performed about this technology	0.6
53	Some literature study shall be performed about this software environment	0.6
54	RS 170 video quality shall be tested and shown to the customer	0.7
55	Data of the system shall be backed up before conversation	0.8
56	Coordination shall be performed with the customer for getting the simulators on time	0.5
57	Coordination shall be performed with the customer for getting the needed CSCI versions on time	0.6
58	The schedule, budget and effort of the project shall be reviewed in terms of the old projects' data	0.8
59	New work force shall be added for documentation	0.9
60	Planning shall be re-done by considering old projects' plan vs actual data	0.8
61	The plan makers shall consider the task assignments of the personnel during planning of the people	0.6
62	Customer shall be convinced to participate in reviews, and follow the project progress	0.5
63	A meeting shall be performed by the participation of all contractors, the coordination shall be decided in this meeting	0.7

Table 14 Organization's Risk Mitigation Actions with Probability for Mitigation Values (cont'd)

64	Customer shall be convinced that if the approval of the document is longer than schedule, then project schedule will be longer	0.5
65	A meeting shall be performed by the participation of all contractors, the coordination shall be decided in this meeting	0.7
66	Project managers shall define project specific metrics, and follow these metrics along the project.	0.8
67	Staff shall receive enough internal training in some areas	0.9
68	Personnel holiday plan shall be prepared in a way that works will finish on time	0.8
69	Training for this CM tool shall be taken by CM Specialist	0.8
70	Training for CM concepts and CM tool shall be taken by CM Specialist	0.8
71	DAR (Decision Analysis & Resolution) procedure shall be written for choosing one of the design alternatives	0.9
72	Project plan and schedule shall be updated in the way that covering trainings	0.9
73	Work plan over the standard working time shall be planned and implemented	0.7
74	Negotiation shall be performed for better schedule with the customer, and negotiation shall be performed for resources with the upper management	0.4
75	Negotiation shall be performed for better schedule with the customer, and negotiation shall be performed for resources with the upper management	0.4
76	The schedule of the project shall be reviewed in terms of the old projects' data, and shall be updated if necessary.	0.6
77	Training for CM concepts shall be taken by CM Specialist	0.8
78	The expectations of the personnel shall be met without creating risks	0.9
79	The expectations of the personnel shall be met without creating risks	0.9
80	Orientation about project status shall be given to added personnel	0.9
81	The expectations of the personnel shall be met without creating risks	0.9
82	The design, needing minimum work effort, shall be chosen.	0.8
83	Tests shall be performed with full coverage, and detected defects shall be corrected until the software passes the tests	0.7
84	Customer shall be convinced that if the approval of the document is longer than schedule, then project schedule will be longer	0.5
85	Addition effort shall be planned and given	0.8
86	The requirements shall be minimized by the negotiations	0.6

Table 14 Organization's Risk Mitigation Actions with Probability for Mitigation Values (cont'd)

87	Contract shall be updated in a way that including the cases for adding/changing/deleting requirements	0.7
88	At the milestone meetings (at the end of system requirement, system design, software requirement, software design and testing phase), the properties/capabilities of the system shall be explained to the customer	0.6
89	Customer shall be encouraged to perform their responsibilities in the customer related process	0.5
90	End users shall be trained by our organization	0.8
91	Coordination shall be performed with the customer for taking necessary preventive actions on this subject	0.5
92	Project schedule and context shall be updated and presented to the customer for the approval	0.6
93	Coordination shall be performed with the customer for CDR meeting and necessary approval made on time	0.5
94	Coordination shall be performed with the customer for getting the data on time	0.5
95	Coordination shall be performed with the customer for getting the MFD hardware on time	0.5
96	Prime Contractor shall be reminded that design decisions should be given before baselined design document	0.5
97	Coordination shall be performed with the Prime Contractor for getting the test tool on time	0.5
98	Coordination shall be performed with the Prime Contractor in order to prevent SDD document being delivered late	0.5
99	Prestudy shall be performed about the necessity of CBS licensing. If necessary, Coordination shall be performed with the Prime Contractor for getting the CBS licensing on time	0.6
100	Coordination shall be performed with the Prime Contractor for getting comment and change requests (if exist) on time	0.5
101	The contacts shall be performed on a certain Prime Contractor	0.6
102	In the suitable platforms, it is said that the project is the first national system in its area	0.7

3.4.4 Risk Prioritization Methods

The intent of the prioritization is to determine the most dangerous risks to which resources for mitigation of risks can be applied with the greatest positive impact to the project. The complete set of risk mitigation actions may not be affordable. A tradeoff analysis should be performed to prioritize the risk mitigation actions for implementation.

Once risks have been identified they should be prioritized for mitigation. Risk Prioritization could be qualitative or quantitative. For the objective prioritization and subject of the thesis, quantitative one is preferred and analyzed in this study.

A relative priority is determined for each risk, based on the asigned risk parameters. There are three offered quantitative methods for prioritization for risk mitigation.

Method 1: Exposure index (as prioritization parameter)

In this method, prioritization parameter is exposure values **[**Probability * Impact**]** of the risk items. Risk items with high exposure value have high prioritization.

This method does not consider

- the resources (costs) expended for the risk mitigation action
- probability that risk mitigation action prevent/reduce risk occurrence/exposure

Method 2: Exposure per cost index (as prioritization parameter)

In this method, prioritization parameter is exposure per cost values **[**Exposure / Risk Mitigation Cost**]** of the risk items. Risk items with high 'exposure per cost' values have high prioritization.

This method is more advanced than method 1, because

- it considers the examination of risk mitigation actions for the benefits they provide versus the resources (costs) they will expend.
- but it does not consider the probability that risk mitigation action prevent/reduce risk occurrence/exposure

Method 3: Expected exposure per cost index (as prioritization parameter)

In this method, prioritization parameter is expected exposure per cost values **[**(Exposure * Probability for Mitigation) / Risk Mitigation Cost**]**. Risk items with high 'expected exposure per cost' values have high prioritization.

This method is the most advanced one, because it considers both

- the examination of risk mitigation actions for the benefits they provide versus the resources (costs) they will expend
- the probability that risk mitigation action prevent/reduce risk occurrence/exposure

3.5. Thresholds

Thresholds should let everybody clearly agree upon whether a risk has become a problem Thresholds can be established to determine acceptability or unacceptability of risks, or triggers for management action. Threshold levels define when a risk becomes unacceptable and triggers the execution of a risk mitigation plan.

Thresholds can be defined for each risk classification or for the whole set of risks. Different approaches for threshold levels can be applied for different risk prioritization methods. After risk prioritization, threshold levels are applied to the prioritized risks.

Risks are monitored and when they exceed the established thresholds, the risk mitigation actions are deployed to return the impacted effort to an acceptable risk level. Since the level of exposure for a given risk changes over time, the risk attributes (probability, impact) should be periodically re-evaluated to determine the risk's importance (risk's prioritization) to the project.

There are three different threshold calculation methods used in this study to provide quantifying risk management.

1. Definition of Threshold 1: Average value of the set – It is calculated as taking the average of the values in the set.
2. Definition of Threshold 2: The value that, covering %50 of the set above it – It is the median of the values in the set.
3. Definition of Threshold 3: Pareto principle for the values in the set – It is the top 20%th of the values in the set.

These three threshold calculation methods are applied for the risks in each class, and for the whole set of risks. Threshold for each classification gives the chance of focusing each class independetly; however, threshold for the whole set gives us the chance of being able to manage risk management activities for the whole set in the organization. It is up to organizations to choose the determination of the thresholds either for the risks in each class or for the whole set of the risks. Both options are covered in this study.

3.6. Road Map for the Study

In this chapter, necessary infrastructure to be able to analyze methods and application data set for quantifying risk management have been prepared. At that point, there are 102 risk items consisting of organization's current risk database plus risk items deriving of using a risk taxonomy. Each risk item has the information of

- class that risk within
- risk probability estimate
- risk impact estimate
- risk exposure value
- risk mitigation action
- risk mitigation cost value
- probability for mitigation estimate

and the determined definitions of

- risk prioritization methods for
    - risk prioritization method 1
    - risk prioritization method 2
    - risk prioritization method 3
- thresholds for
    - threshold 1
    - threshold 2
    - threshold 3

CHAPTER 4

DISCUSSION

In this chapter, at first conceptual structure is built to use in making decisions in quantifying risk management, and the results of the structure on the data set of risk items defined in Chapter 3 are disscussed. In the rest of the Chapter, quantifying risk management policies are compared by finding out and analyzing their performance with respect to designated preference profiles defined below. In other words, the defined policies are ranked for different preference profiles.

Here, the main aim is to provide guidance on the effects of employing different risk management policies for different profiles.

Namely, the four aspects; risk items mitigated, exposures prevented, costs, and expected exposures prevented are examined for various quantifying risk management policies. These are the main issue for whom quantifying objectives are designated and against which quantifying risk management's actual performance is monitored.

4.1. Policies

The organizations need policies to be able to use in decision making in quantifying risk management.

Three threshold calculation methods for each risk prioritization method are applied for the risks in each class, and for the whole set of risks. Threshold for each classification gives the chance of focusing each class independetly; however, threshold for the whole set gives us the chance of being able to manage risk management activities for the whole set in the organization. It is up to organizations to choose the determination of the thresholds either for the risks in each class or

forthe whole set of the risks. Both options are covered in this study. The set of policies for this study is defined in Table 15.

- There are 3 different Risk Prioritization Methods defined above
  - Risk Prioritization Method 1
  - Risk Prioritization Method 2
  - Risk Prioritization Method 3
- There are 2 different ways to run the quantifying risk management
  - Apply to the each class of risks, then get their summation
  - Apply to the whole set of risks
- There are 3 different Thresholds definitions defined above
  - Threshold 1
  - Threshold 2
  - Threshold 3

Therefore, there are 3*2*3 = 18 policies in the set. These are explained in Table 15.

Table 15 Risk Management Policies Considered in the Study

POLICY	RISK PRIORITIZATION METHOD	APPLY TO	THRESHOLD
“Policy 1” includes	Method 1	Each Class of Risks	Threshold 1
“Policy 2” includes	Method 1	Each Class of Risks	Threshold 2
“Policy 3” includes	Method 1	Each Class of Risks	Threshold 3
“Policy 4” includes	Method 1	Whole Set of Risks	Threshold 1
“Policy 5” includes	Method 1	Whole Set of Risks	Threshold 2
“Policy 6” includes	Method 1	Whole Set of Risks	Threshold 3
“Policy 7” includes	Method 2	Each Class of Risks	Threshold 1
“Policy 8” includes	Method 2	Each Class of Risks	Threshold 2

Table 15 Risk Management Policies Considered in the Study (cont’d)

“Policy 9” includes	Method 2	Each Class of Risks	Threshold 3
“Policy 10” includes	Method 2	Whole Set of Risks	Threshold 1
“Policy 11” includes	Method 2	Whole Set of Risks	Threshold 2
“Policy 12” includes	Method 2	Whole Set of Risks	Threshold 3
“Policy 13” includes	Method 3	Each Class of Risks	Threshold 1
“Policy 14” includes	Method 3	Each Class of Risks	Threshold 2
“Policy 15” includes	Method 3	Each Class of Risks	Threshold 3
“Policy 16” includes	Method 3	Whole Set of Risks	Threshold 1
“Policy 17” includes	Method 3	Whole Set of Risks	Threshold 2
“Policy 18” includes	Method 3	Whole Set of Risks	Threshold 3

4.2. Profiles

Profiles for quantifying risk management correspond to relative importance of risk items mitigated, exposures prevented, costs, and expected exposures prevented due to varying preferences shaped according to organizational policies and project structure.

Each profile in the profile set highlights a decision parameter. These decision parameters are either based decision parameters or derived decision parameters.

Based Decision Parameters:

- # of risk items mitigated
- # of risk items monitored
- total exposure prevented for mitigated risks
- total exposure released for monitored risks
- risk mitigation costs for mitigated risks (man-hour)
- potential risk mitigation costs for monitored risks (man-hour)
- total expected exposure prevented for mitigated risks
- total expected exposure released for monitored risks

Derived Decision Parameters:

- percentage of risk items mitigated
- percentage of total exposure prevented
- percentage of risk mitigation costs
- percentage of total expected exposure prevented
- (total exposure prevented for mitigated risks) / (# of risk items mitigated)
- (risk mitigation costs for mitigated risks) / (# of risk items mitigated)
- (total expected exposure prevented for mitigated risks) / (# of risk items mitigated)
- (total exposure prevented for mitigated risks) / (risk mitigation costs for mitigated risks)
- (total expected exposure prevented for mitigated risks) / (risk mitigation costs for mitigated risks)

The profiles highlighting a characteristic of a certain decision parameter are given at Table 16.

Table 16 Profiles Considered in the Study

PROFILE	DECISION PARAMETER
Profile 1 seeks for	Maximum of "# of risk items mitigated" (minimum of "# of risk items monitored")
Profile 2 seeks for	Minimum of "# of risk items mitigated" (maximum of "# of risk items monitored")
Profile 3 seeks for	Maximum of "percentage of risk items mitigated"
Profile 4 seeks for	Minimum of "percentage of risk items mitigated"
Profile 5 seeks for	Maximum of "total exposure prevented for mitigated risks" (minimum of "total exposure released for monitored risks")
Profile 6 seeks for	Maximum of "percentage of total exposure prevented"
Profile 7 seeks for	Minimum of "risk mitigation costs for mitigated risks in man-hour" (maximum of "potential risk mitigation costs for monitored risks in man-hour")
Profile 8 seeks for	Minimum of "percentage of risk mitigation costs"

Table 16 Profiles Considered in the Study (cont'd)

Profile 9 seeks for	Maximum of "total expected exposure prevented for mitigated risks" (minimum of "total expected exposure released for monitored risks")
Profile 10 seeks for	Maximum of "percentage of total expected exposure prevented"
Profile 11 seeks for	Maximum of "total exposure prevented for mitigated risks / # of risk items mitigated"
Profile 12 seeks for	Minimum of "risk mitigation costs for mitigated risks / # of risk items mitigated"
Profile 13 seeks for	Maximum of "total expected exposure prevented for mitigated risks / # of risk items mitigated"
Profile 14 seeks for	Maximum of "total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks"
Profile 15 seeks for	Maximum of "total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks"

The software organizations working for the avionic systems can be an example of Profile 5, because it is a mission critical system that most of the exposures should be prevented. The software organizations with small budget for risk management can be an example of Profile 7 which aims to minimize risk mitigation costs. A software organization aims to have effective risk management is a good example for Profile 14 which provides maximum prevention of total expected exposure per same unit of cost.

4.3. Application of Policies

In this section, I shall apply the policies to the data set of risk items formed in Chapter 3. The content of the policies is given in Table 15. The content of the policies consist of the followings:

- The definitions of Risk Prioritization Methods given in Section 3.4.4.
- Usage of the classification for the risks given in Table 6.
- The definitions of Thresholds given in Section 3.5.

Policy 1, 2, 3, 4, 5, and 6 use Risk Prioritization Method 1. Risk Prioritization Method 1 is based on "exposure" values of the risk items. Therefore, three threshold definitions for these policies are in the followings:

- Threshold 1: Average exposure value – It is calculated as taking the average of exposure values in the set.
- Threshold 2: The exposure value that, covering %50 of the set above it – It is the median of exposure values in the set.
- Threshold 3: Pareto principle for exposure values – It is the top 20%th of the exposure values in the set.

Policy 7, 8, 9, 10, 11, and 12 use Risk Prioritization Method 2. Risk Prioritization Method 2 is based on "exposure/risk mitigation cost" values of the risk items. Therefore, three threshold definitions for these policies are in the followings:

- Threshold 1: Average "exposure/risk mitigation cost" value – It is calculated as taking the average of "exposure/risk mitigation cost" values in the set.
- Threshold 2: The "exposure/risk mitigation cost" value that, covering %50 of the set above it – It is the median of "exposure/risk mitigation cost" values in the set.
- Threshold 3: Pareto principle for "exposure/risk mitigation cost" values – It is the top 20%th of the "exposure/risk mitigation cost" values in the set.

Policy 13, 14, 15, 16, 17, and 18 use Risk Prioritization Method 3. Risk Prioritization Method 3 is based on "(exposure * probability for mitigation) / risk mitigation cost" values of the risk items. Therefore, three threshold definitions for these policies are in the followings:

- Threshold 1: Average "(exposure * probability for mitigation) / risk mitigation cost" value – It is calculated as taking the average of "(exposure * probability for mitigation) / risk mitigation cost" values in the set.
- Threshold 2: The "(exposure * probability for mitigation) / risk mitigation cost" value that, covering %50 of the set above it – It is the median of "(exposure * probability for mitigation) / risk mitigation cost" values in the set.

- Threshold 3: Pareto principle for "(exposure * probability for mitigation) / risk mitigation cost" values – It is the top 20%th of the "(exposure * probability for mitigation) / risk mitigation cost" values in the set.

4.3.1 Policy 1-6

"Product Engineering" Class:

There are 42 risk items in this class. According to Risk Prioritization Method 1, the prioritization of these 42 risk items can be seen in Table 22 at Appendix C.

After three different threshold calculation methods applied to the risks within "Product Engineering" class (Table 22), the values for threshold levels are;

Threshold 1 = **2.53** (the average of the exposure values in Table 22)

Threshold 2 = **2.25** (the median of the exposure values in Table 22)

Threshold 3 = **4.20** (the pareto principle point of the exposure values in Table 22)

In Figure 3 at Appendix D, there is the distribution of exposure values of the risks within "Product Enginieering" class, sorted in accordance with Risk Prioritization Method 1.

If **Policy 1** is applied, as we see in Table 22

- Risk Mitigation Actions shall be performed for **18** of 42 risk items. Risks with # '1', '5', '25', '6', '36', '10', '15', '33', '2', '9', '21', '32', '4', '19', '31', '23', '37', and '39' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **24** of 42 risk items. Risks with # '24', '3', '11', '29', '38', '13', '14', '26', '34', '7', '12', '30', '41', '20', '35', '16', '18', '42', '28', '22', '27', '40', '8', and '17' shall be monitored.
- Risk Mitigation Costs are **1448 man-hours** for these 18 mitigated risk items.
- Risk Mitigation Costs would be **1256 man-hours** for these monitored 24 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 18 risk mitigation actions is **1.492**
- Total exposure (deterministic exposure) per man-hour released by not performing 24 risk mitigation actions is **1.106**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 18 risk mitigation actions is **0.932**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 24 risk mitigation actions is **0.691**

If **Policy 2** is applied, as we see in Table 22

- Risk Mitigation Actions shall be performed for **21** of 42 risk items. Risks with # '1', '5', '25', '6', '36', '10', '15', '33', '2', '9', '21', '32', '4', '19', '31', '23', '37', '39', '24', '3', and '11' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **21** of 42 risk items. Risks with # '29', '38', '13', '14', '26', '34', '7', '12', '30', '41', '20', '35', '16', '18', '42', '28', '22', '27', '40', '8', and '17' shall be monitored.
- Risk Mitigation Costs are **1744 man-hours** for these 21 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **960 man-hours** for these monitored 21 risk items.
- Total exposure (deterministic exposure) per man-hour prevented by performing 21 risk mitigation actions is **1.618**
- Total exposure (deterministic exposure) per man-hour released by not performing 21 risk mitigation actions is **0.980**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 21 risk mitigation actions is **1.018**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 21 risk mitigation actions is **0.605**

If **Policy 3** is applied, as we see in Table 22

- Risk Mitigation Actions shall be performed for **8** of 42 risk items. Risks with # '1', '5', '25', '6', '36', '10', '15', and '33' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **34** of 42 risk items. Risks with # '2', '9', '21', '32', '4', '19', '31', '23', '37', '39', '24' '3', '11', '29', '38', '13', '14', '26', '34', '7', '12', '30', '41', '20', '35', '16', '18', '42', '28', '22', '27', '40', '8', and '17' shall be monitored.
- Risk Mitigation Costs are **664 man-hours** for these 8 mitigated risk items.
- Risk Mitigation Costs would be **2040 man-hours** for these monitored 34 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 8 risk mitigation actions is **0.804**
- Total exposure (deterministic exposure) per man-hour released by not performing 34 risk mitigation actions is **1.794**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 8 risk mitigation actions is **0.526**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 34 risk mitigation actions is **1.098**

"Development Environment" Class:

There are 29 risk items in this class. According to Risk Prioritization Method 1, the prioritization of these 29 items can be seen in Table 23 at Appendix C.

After three different threshold calculation methods applied to the risks within "Development Environment" class (Table 23), the values for threshold levels are;

Threshold 1 = **2.94** (the average of the exposure values in Table 23)

Threshold 2 = **2.80** (the median of the exposure values in Table 23)

Threshold 3 = **4.20** (the pareto principle point of the exposure values in Table 23)

In Figure 4 at Appendix D, there is the distribution of exposure values of the risks within "Development Environment" class, sorted in accordance with Risk Prioritization Method 1.

If **Policy 1** is applied, as we see in Table 23

- Risk Mitigation Actions shall be performed for **14** of 29 risk items. Risks with # '59', '69', '70', '58', '60', '67', '43', '54', '57', '49', '53', '62', '48', and '56' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **15** of 29 risk items. Risks with # '63', '61', '64', '45', '55', '46', '65', '50', '52', '44', '47', '51', '66', '71', and '68' shall be monitored.
- Risk Mitigation Costs are **759 man-hours** for these 14 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **468 man-hours** for these monitored 15 risk items.
- Total exposure (deterministic exposure) per man-hour prevented by performing 14 risk mitigation actions is **1.839**
- Total exposure (deterministic exposure) per man-hour released by not performing 15 risk mitigation actions is **1.163**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 14 risk mitigation actions is **1.256**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 15 risk mitigation actions is **0.834**

If **Policy 2** is applied, as we see in Table 23

- Risk Mitigation Actions shall be performed for **15** of 29 risk items. Risks with # '59', '69', '70', '58', '60', '67', '43', '54', '57', '49', '53', '62', '48', '56', and '63' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **14** of 29 risk items. Risks with # '61', '64', '45', '55', '46', '65', '50', '52', '44', '47', '51', '66', '71', and '68' shall be monitored.
- Risk Mitigation Costs are **799 man-hours** for these 15 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **428 man-hours** for these monitored 14 risk items.

- Total exposure (deterministic exposure) per man-hour prevented by performing 15 risk mitigation actions is **1.909**
- Total exposure (deterministic exposure) per man-hour released by not performing 14 risk mitigation actions is **1.093**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 15 risk mitigation actions is **1.305**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 14 risk mitigation actions is **0.785**

If **Policy 3** is applied, as we see in Table 23

- Risk Mitigation Actions shall be performed for **6** of 29 risk items. Risks with # '59', '69', '70', '58', '60', and '67', shall be mitigated.
- Risk Mitigation Actions shall not be performed for **23** of 29 risk items. Risks with # '43', '54', '57', '49', '53', '62', '48', '56', '63', '61', '64', '45', '55', '46', '65', '50', '52', '44', '47', '51', '66', '71', and '68' shall be monitored.
- Risk Mitigation Costs are **375 man-hours** for these 6 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **852 man-hours** for these monitored 23 risk items.
- Total exposure (deterministic exposure) per man-hour prevented by performing 6 risk mitigation actions is **0.805**
- Total exposure (deterministic exposure) per man-hour released by not performing 23 risk mitigation actions is **2.197**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 6 risk mitigation actions is **0.653**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 23 risk mitigation actions is **1.436**

"Program Constraints" Class:

There are 31 risk items in this class. According to Risk Prioritization Method 1, the prioritization of these 31 items can be seen in Table 24 at Appendix C.

After three different threshold calculation methods applied to the risks within "Program Constraints" class (Table 24), the values for threshold levels are;

Threshold 1 = **3.15** (the average of the exposure values in Table 24)

Threshold 2 = **3.00** (the median of the exposure values in Table 24)

Threshold 3 = **4.20** (the pareto principle point of the exposure values in Table 24)

In Figure 5 at Appendix D, there is the distribution of exposure values of the risks within "Program Constraints" class, sorted in accordance with Risk Prioritization Method 1.

If **Policy 1** is applied, as we see in Table 24

- Risk Mitigation Actions shall be performed for **15** of 31 risk items. Risks with # ‘85’, ‘101’, ‘73’, ‘94’, ‘87’, ‘77’, ‘88’, ‘79’, ‘92’, ‘74’, ‘78’, ‘86’, ‘95’, ‘97’and ‘93’ shall be mitigated.
- Risk Mitigation Actions shall not be performed for **16** of 31 risk items. Risks with # ‘75’, ‘100’, ‘76’, ‘96’, ‘81’, ‘91’, ‘72’, ‘82’, ‘84’, ‘90’, ‘99’, ‘83’, ‘89’, ‘98’, ‘80’, and ‘102’ shall be monitored.
- Risk Mitigation Costs are **898 man-hours** for these 15 mitigated risk items. (After converting of YTL to man-hour by ‘1 man-hour = 15 YTL’)
- Risk Mitigation Costs would be **565 man-hours** for these monitored 16 risk items. (After converting of YTL to man-hour by ‘1 man-hour = 15 YTL’)
- Total exposure (deterministic exposure) per man-hour prevented by performing 15 risk mitigation actions is **2.388**
- Total exposure (deterministic exposure) per man-hour released by not performing 16 risk mitigation actions is **1.631**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 15 risk mitigation actions is **1.400**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 16 risk mitigation actions is **0.995**

If **Policy 2** is applied, as we see in Table 24

- Risk Mitigation Actions shall be performed for **17** of 31 risk items. Risks with # ‘85’, ‘101’, ‘73’, ‘94’, ‘87’, ‘77’, ‘88’, ‘79’, ‘92’, ‘74’, ‘78’, ‘86’, ‘95’, ‘97’, ‘93’, ‘75’, and ‘100’ shall be mitigated.
- Risk Mitigation Actions shall not be performed for **14** of 31 risk items. Risks with # ‘76’, ‘96’, ‘81’, ‘91’, ‘72’, ‘82’, ‘84’, ‘90’, ‘99’, ‘83’, ‘89’, ‘98’, ‘80’, and ‘102’ shall be monitored.
- Risk Mitigation Costs are **938 man-hours** for these 17 mitigated risk items. (After converting of YTL to man-hour by ‘1 man-hour = 15 YTL’)
- Risk Mitigation Costs would be **525 man-hours** for these monitored 14 risk items. (After converting of YTL to man-hour by ‘1 man-hour = 15 YTL’)
- Total exposure (deterministic exposure) per man-hour prevented by performing 17 risk mitigation actions is **2.700**
- Total exposure (deterministic exposure) per man-hour released by not performing 14 risk mitigation actions is **1.319**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 17 risk mitigation actions is **1.544**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 14 risk mitigation actions is **0.851**

If **Policy 3** is applied, as we see in Table 24

- Risk Mitigation Actions shall be performed for **7** of 31 risk items. Risks with # ‘85’, ‘101’, ‘73’, ‘94’, ‘87’, ‘77’, and ‘88’shall be mitigated.
- Risk Mitigation Actions shall not be performed for **24** of 31 risk items. Risks with # ‘79’, ‘92’, ‘74’, ‘78’, ‘86’, ‘95’, ‘97’, ‘93’, ‘75’, ‘100’, ‘76’, ‘96’, ‘81’, ‘91’, ‘72’, ‘82’, ‘84’, ‘90’, ‘99’, ‘83’, ‘89’, ‘98’, ‘80’, and ‘102’ shall be monitored.

- Risk Mitigation Costs are **360 man-hours** for these 7 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **1104 man-hours** for these monitored 24 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 7 risk mitigation actions is **1.273**
- Total exposure (deterministic exposure) per man-hour released by not performing 24 risk mitigation actions is **2.746**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 7 risk mitigation actions is **0.899**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 24 risk mitigation actions is **1.580**

"Whole Set of Risks":

There are 102 risk items in the whole set. According to Risk Prioritization Method 1, the prioritization of these 102 items can be seen in Table 25 at Appendix C.

After three different threshold calculation methods applied to the whole set of risks (Table 25), the values for threshold levels are;

Threshold 1 = **2.83** (the average of the exposure values in Table 25)

Threshold 2 = **2.50** (the median of the exposure values in Table 25)

Threshold 3 = **4.20** (the pareto principle point of the exposure values in Table 25)

In Figure 6 at Appendix D, there is the distribution of exposure values of the whole set of risks, sorted in accordance with Risk Prioritization Method 1.

If **Policy 4** is applied, as we see in Table 25

- Risk Mitigation Actions shall be performed for **46** of 102 risk items. Risks with # '59', '85', '1', '5', '101', '25', '69', '70', '73', '94', '6', '58', '60', '87', '36', '10', '15', '33', '67', '77', '88', '79', '92', '2', '9', '43', '54', '57', '74', '78', '86', '95', '97', '21', '32', '49', '53', '62', '93', '4', '19', '31', '48', '56', '75', and '100' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **56** of 102 risk items. Risks with # '23', '37', '39', '63', '24', '61', '64', '76', '3', '11', '45', '55', '96', '29', '81', '38', '91', '13', '14', '26', '34', '46', '65', '72', '82', '84', '90', '7', '50', '99', '12', '30', '41', '52', '83', '89', '98', '20', '35', '44', '47', '16', '18', '42', '51', '80', '102', '28', '66', '71', '22', '27', '40', '68', '8', and '17' shall be monitored.
- Risk Mitigation Costs are **2989 man-hours** for these 46 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **2425 man-hours** for these monitored 56 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')

- Total exposure (deterministic exposure) per man-hour prevented by performing 46 risk mitigation actions is **5.786**
- Total exposure (deterministic exposure) per man-hour released by not performing 56 risk mitigation actions is **3.833**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 46 risk mitigation actions is **3.596**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 56 risk mitigation actions is **2.512**

If **Policy 5** is applied, as we see in Table 25

- Risk Mitigation Actions shall be performed for **54** of 102 risk items. Risks with # '59', '85', '1', '5', '101', '25', '69', '70', '73', '94', '6', '58', '60', '87', '36', '10', '15', '33', '67', '77', '88', '79', '92', '2', '9', '43', '54', '57', '74', '78', '86', '95', '97', '21', '32', '49', '53', '62', '93', '4', '19', '31', '48', '56', '75', '100', '23', '37', '39', '63', '24', '61', '64', and '76' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **48** of 102 risk items. Risks with # '3', '11', '45', '55', '96', '29', '81', '38', '91', '13', '14', '26', '34', '46', '65', '72', '82', '84', '90', '7', '50', '99', '12', '30', '41', '52', '83', '89', '98', '20', '35', '44', '47', '16', '18', '42', '51', '80', '102', '28', '66', '71', '22', '27', '40', '68', '8', and '17' shall be monitored.
- Risk Mitigation Costs are **3357 man-hours** for these 54 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **2057 man-hours** for these monitored 48 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 54 risk mitigation actions is **6.437**
- Total exposure (deterministic exposure) per man-hour released by not performing 48 risk mitigation actions is **3.182**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 54 risk mitigation actions is **3.967**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 48 risk mitigation actions is **2.141**

If **Policy 6** is applied, as we see in Table 25

- Risk Mitigation Actions shall be performed for **21** of 102 risk items. Risks with # '59', '85', '1', '5', '101', '25', '69', '70', '73', '94', '6', '58', '60', '87', '36', '10', '15', '33', '67', '77', and '88'shall be mitigated.
- Risk Mitigation Actions shall not be performed for **81** of 102 risk items. Risks with # '79', '92', '2', '9', '43', '54', '57', '74', '78', '86', '95', '97', '21', '32', '49', '53', '62', '93', '4', '19', '31', '48', '56', '75', '100', '23', '37', '39', '63', '24', '61', '64', '76', '3', '11', '45', '55', '96', '29', '81', '38', '91', '13', '14', '26', '34', '46', '65', '72', '82', '84', '90', '7', '50', '99', '12', '30', '41', '52', '83', '89', '98', '20', '35', '44', '47', '16', '18', '42', '51', '80', '102', '28', '66', '71', '22', '27', '40', '68', '8', and '17' shall be monitored.
- Risk Mitigation Costs are **1399 man-hours** for these 21 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')

- Risk Mitigation Costs would be **3996 man-hours** for these monitored 81 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 21 risk mitigation actions is **2.882**
- Total exposure (deterministic exposure) per man-hour released by not performing 81 risk mitigation actions is **6.737**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 21 risk mitigation actions is **1.994**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 81 risk mitigation actions is **4.114**

4.3.2 Policy 7-12

"Product Engineering" Class:

There are 42 risk items in this class. According to Risk Prioritization Method 2, the prioritization of these 42 risk items can be seen in Table 26 at Appendix C.

After three different threshold calculation methods applied to the risks within "Product Engineering" class (Table 26), the values for threshold levels are;

Threshold 1 = **0.062** (the average of the "exposure/risk mitigation cost" values in Table 26)

Threshold 2 = **0.038** (the median of the "exposure/risk mitigation cost" values in Table 26)

Threshold 3 = **0.084** (the pareto principle point of the "exposure/risk mitigation cost" values in Table 26)

In Figure 7 at Appendix D, there is the distribution of "exposure/risk mitigation cost" values of the risks within "Product Enginieering" class, sorted in accordance with Risk Prioritization Method 2.

If **Policy 7** is applied, as we see in Table 26

- Risk Mitigation Actions shall be performed for **12** of 42 risk items. Risks with # '1', '29', '4', '23', '10', '15', '20', '25', '13', '3', '2', and '21' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **30** of 42 risk items. Risks with # '28', '33', '14', '12', '26', '8', '24', '5', '36', '16', '22', '32', '37', '39', '34', '6', '9', '38', '19', '17', '30', '41', '7', '35', '31', '27', '18', '42', '11', and '40' shall be monitored.
- Risk Mitigation Costs are **368 man-hours** for these 12 mitigated risk items.

- Risk Mitigation Costs would be **2336 man-hours** for these monitored 30 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 12 risk mitigation actions is **1.667**
- Total exposure (deterministic exposure) per man-hour released by not performing 30 risk mitigation actions is **0.930**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 12 risk mitigation actions is **0.906**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 30 risk mitigation actions is **0.717**

If **Policy 8** is applied, as we see in Table 26

- Risk Mitigation Actions shall be performed for **23** of 42 risk items. Risks with # '1', '29', '4', '23', '10', '15', '20', '25', '13', '3', '2', '21', '28', '33', '14', '12', '26', '8', '24', '5', '36', '16', and '22' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **19** of 42 risk items. Risks with # '32', '37', '39', '34', '6', '9', '38', '19', '17', '30', '41', '7', '35', '31', '27', '18', '42', '11', and '40' shall be monitored.
- Risk Mitigation Costs are **972 man-hours** for these 23 mitigated risk items.
- Risk Mitigation Costs would be **1732 man-hours** for these monitored 19 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 23 risk mitigation actions is **2.147**
- Total exposure (deterministic exposure) per man-hour released by not performing 19 risk mitigation actions is **0.451**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 23 risk mitigation actions is **1.285**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 19 risk mitigation actions is **0.338**

If **Policy 9** is applied, as we see in Table 26

- Risk Mitigation Actions shall be performed for **8** of 42 risk items. Risks with # '1', '29', '4', '23', '10', '15', '20', and '25' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **34** of 42 risk items. Risks with # '13', '3', '2', '21', '28', '33', '14', '12', '26', '8', '24', '5' '36', '16', '22', '32', '37', '39', '34', '6', '9', '38', '19', '17', '30', '41', '7', '35', '31', '27', '18', '42', '11', and '40' shall be monitored.
- Risk Mitigation Costs are **216 man-hours** for these 8 mitigated risk items.
- Risk Mitigation Costs would be **2488 man-hours** for these monitored 34 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 8 risk mitigation actions is **1.363**
- Total exposure (deterministic exposure) per man-hour released by not performing 34 risk mitigation actions is **1.235**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 8 risk mitigation actions is **0.709**

- Total expected exposure (probabilistic exposure) per man-hour released by not performing 34 risk mitigation actions is **0.915**

"Development Environment" Class:

There are 29 risk items in this class. According to Risk Prioritization Method 2, the prioritization of these 29 risk items can be seen in Table 27 at Appendix C.

After three different threshold calculation methods applied to the risks within "Development Environment" class (Table 27), the values for threshold levels are;

Threshold 1 = **0.104** (the average of the "exposure/risk mitigation cost" values in Table 27)

Threshold 2 = **0.070** (the median of the "exposure/risk mitigation cost" values in Table 27)

Threshold 3 = **0.200** (the pareto principle point of the "exposure/risk mitigation cost" values in Table 27)

In Figure 8 at Appendix D, there is the distribution of "exposure/risk mitigation cost" values of the risks within "Development Environment" class, sorted in accordance with Risk Prioritization Method 2.

If **Policy 7** is applied, as we see in Table 27

- Risk Mitigation Actions shall be performed for **11** of 29 risk items. Risks with # '55', '69', '57', '49', '62', '70', '56', '64', '58', '60', and '50' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **18** of 29 risk items. Risks with # '61', '68', '54', '63', '46', '45', '53', '59', '65', '44', '51', '67', '47', '43', '48', '66', '52', and '71' shall be monitored.
- Risk Mitigation Costs are **231 man-hours** for these 11 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **996 man-hours** for these monitored 18 risk items.
- Total exposure (deterministic exposure) per man-hour prevented by performing 11 risk mitigation actions is **2.128**
- Total exposure (deterministic exposure) per man-hour released by not performing 18 risk mitigation actions is **0.875**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 11 risk mitigation actions is **1.412**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 18 risk mitigation actions is **0.678**

If **Policy 8** is applied, as we see in Table 27

- Risk Mitigation Actions shall be performed for **15** of 29 risk items. Risks with # ‘55’, ‘69’, ‘57’, ‘49’, ‘62’, ‘70’, ‘56’, ‘64’, ‘58’, ‘60’, ‘50’, ‘61’, ‘68’, ‘54’, and ‘63’ shall be mitigated.
- Risk Mitigation Actions shall not be performed for **14** of 29 risk items. Risks with #, ‘46’, ‘45’, ‘53’, ‘59’, ‘65’, ‘44’, ‘51’, ‘67’, ‘47’, ‘43’, ‘48’, ‘66’, ‘52’, and ‘71’ shall be monitored.
- Risk Mitigation Costs are **359 man-hours** for these 15 mitigated risk items. (After converting of YTL to man-hour by ‘1 man-hour = 15 YTL’)
- Risk Mitigation Costs would be **868 man-hours** for these monitored 14 risk items.
- Total exposure (deterministic exposure) per man-hour prevented by performing 15 risk mitigation actions is **2.424**
- Total exposure (deterministic exposure) per man-hour released by not performing 14 risk mitigation actions is **0.579**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 15 risk mitigation actions is **1.619**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 14 risk mitigation actions is **0.471**

If **Policy 9** is applied, as we see in Table 27

- Risk Mitigation Actions shall be performed for **6** of 29 risk items. Risks with # ‘55’, ‘69’, ‘57’, ‘49’, ‘62’, and ‘70’ shall be mitigated.
- Risk Mitigation Actions shall not be performed for **23** of 29 risk items. Risks with # ‘56’, ‘64’, ‘58’, ‘60’, ‘50’, ‘61’, ‘68’, ‘54’, ‘63’, ‘46’, ‘45’, ‘53’, ‘59’, ‘65’, ‘44’, ‘51’, ‘67’, ‘47’, ‘43’, ‘48’, ‘66’, ‘52’, and ‘71’ shall be monitored.
- Risk Mitigation Costs are **103 man-hours** for these 6 mitigated risk items. (After converting of YTL to man-hour by ‘1 man-hour = 15 YTL’)
- Risk Mitigation Costs would be **1124 man-hours** for these monitored 23 risk items.
- Total exposure (deterministic exposure) per man-hour prevented by performing 6 risk mitigation actions is **1.426**
- Total exposure (deterministic exposure) per man-hour released by not performing 23 risk mitigation actions is **1.576**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 6 risk mitigation actions is **0.988**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 23 risk mitigation actions is **1.102**

“Program Constraints” Class:

There are 31 risk items in this class. According to Risk Prioritization Method 2, the prioritization of these 31 risk items can be seen in Table 28 at Appendix C.

After three different threshold calculation methods applied to the risks within “Program Constraints” class (Table 28), the values for threshold levels are;

Threshold 1 = **0.130** (the average of the "exposure/risk mitigation cost" values in Table 28)

Threshold 2 = **0.125** (the median of the "exposure/risk mitigation cost" values in Table 28)

Threshold 3 = **0.219** (the pareto principle point of the "exposure/risk mitigation cost" values in Table 28)

In Figure 9 at Appendix D, there is the distribution of "exposure/risk mitigation cost" values of the risks within "Program Constraints" class, sorted in accordance with Risk Prioritization Method 2.

If **Policy 7** is applied, as we see in Table 28

- Risk Mitigation Actions shall be performed for **12** of 31 risk items. Risks with # '73', '94', '82', '95', '97', '93', '100', '101', '92', '96', '74', and '91' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **19** of 31 risk items. Risks with # '75', '72', '84', '89', '86', '77', '87', '98', '99', '76', '88', '90', '80', '102', '85', '83', '79', '78', and '81' shall be monitored.
- Risk Mitigation Costs are **212 man-hours** for these 12 mitigated risk items.
- Risk Mitigation Costs would be **1252 man-hours** for these monitored 19 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 12 risk mitigation actions is **2.650**
- Total exposure (deterministic exposure) per man-hour released by not performing 19 risk mitigation actions is **1.369**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 12 risk mitigation actions is **1.510**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 19 risk mitigation actions is **0.886**

If **Policy 8** is applied, as we see in Table 28

- Risk Mitigation Actions shall be performed for **16** of 31 risk items. Risks with # '73', '94', '82', '95', '97', '93', '100', '101', '92', '96', '74', '91', '75', '72', '84', and '89' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **15** of 31 risk items. Risks with # '86', '77', '87', '98', '99', '76', '88', '90', '80', '102', '85', '83', '79', '78', and '81' shall be monitored.
- Risk Mitigation Costs are **280 man-hours** for these 16 mitigated risk items.
- Risk Mitigation Costs would be **1184 man-hours** for these monitored 15 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 16 risk mitigation actions is **3.150**

- Total exposure (deterministic exposure) per man-hour released by not performing 15 risk mitigation actions is **0.869**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 16 risk mitigation actions is **1.797**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 15 risk mitigation actions is **0.598**

If **Policy 9** is applied, as we see in Table 28

- Risk Mitigation Actions shall be performed for **6** of 31 risk items. Risks with # '73', '94', '82', '95', '97', and '93' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **25** of 31 risk items. Risks with # '100', '101', '92', '96', '74', '91', '75', '72', '84', '89', '86', '77', '87', '98', '99', '76', '88', '90', '80', '102', '85', '83', '79', '78', and '81' shall be monitored.
- Risk Mitigation Costs are **84 man-hours** for these 6 mitigated risk items.
- Risk Mitigation Costs would be **1380 man-hours** for these monitored 25 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 6 risk mitigation actions is **1.694**
- Total exposure (deterministic exposure) per man-hour released by not performing 25 risk mitigation actions is **2.325**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 6 risk mitigation actions is **1.012**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 25 risk mitigation actions is **1.467**

"Whole Set of Risks":

There are 102 risk items in the whole set. According to Risk Prioritization Method 2, the prioritization of these 102 risk items can be seen in Table 29 at Appendix C.

After three different threshold calculation methods applied to the whole set of risks (Table 29), the values for threshold levels are;

Threshold 1 = **0.094** (the average of the "exposure/risk mitigation cost" values in Table 29)

Threshold 2 = **0.059** (the median of the "exposure/risk mitigation cost" values in Table 29)

Threshold 3 = **0.167** (the pareto principle point of the "exposure/risk mitigation cost" values in Table 29)

In Figure 10 at Appendix D, there is the distribution of "exposure/risk mitigation cost" values of the whole set of risks, sorted in accordance with Risk Prioritization Method 2.

If **Policy 10** is applied, as we see in Table 29

- Risk Mitigation Actions shall be performed for **38** of 102 risk items. Risks with # '73', '1', '94', '55', '69', '29', '82', '57', '95', '97', '49', '62', '93', '70', '4', '56', '100', '101', '23', '92', '64', '96', '74', '91', '75', '72', '84', '89', '58', '60', '50', '86', '10', '15', '77', '87', '98', and '20' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **64** of 102 risk items. Risks with # '25', '13', '61', '3', '99', '68', '2', '54', '21', '63', '76', '46', '45', '88', '28', '53', '59', '33', '14', '65', '90', '80', '102', '12', '44', '85', '51', '26', '8', '24', '5', '36', '67', '16', '22', '32', '37', '39', '47', '43', '48', '34', '6', '9', '66', '38', '19', '17', '30', '41', '52', '7', '71', '83', '35', '79', '31', '27', '78', '18', '42', '11', '81', and '40' shall be monitored.
- Risk Mitigation Costs are **779 man-hours** for these 38 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **4616 man-hours** for these monitored 64 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 38 risk mitigation actions is **6.966**
- Total exposure (deterministic exposure) per man-hour released by not performing 64 risk mitigation actions is **2.652**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 38 risk mitigation actions is **4.127**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 64 risk mitigation actions is **1.982**

If **Policy 11** is applied, as we see in Table 29

- Risk Mitigation Actions shall be performed for **51** of 102 risk items. Risks with # '73', '1', '94', '55', '69', '29', '82', '57', '95', '97', '49', '62', '93', '70', '4', '56', '100', '101', '23', '92', '64', '96', '74', '91', '75', '72', '84', '89', '58', '60', '50', '86', '10', '15', '77', '87', '98', '20', '25', '13', '61', '3', '99', '68', '2', '54', '21', '63', '76', '46', and '45' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **51** of 102 risk items. Risks with # '88', '28', '53', '59', '33', '14', '65', '90', '80', '102', '12', '44', '85', '51', '26', '8', '24', '5', '36', '67', '16', '22', '32', '37', '39', '47', '43', '48', '34', '6', '9', '66', '38', '19', '17', '30', '41', '52', '7', '71', '83', '35', '79', '31', '27', '78', '18', '42', '11', '81', and '40' shall be monitored.
- Risk Mitigation Costs are **1259 man-hours** for these 51 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **4136 man-hours** for these monitored 51 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')

- Total exposure (deterministic exposure) per man-hour prevented by performing 51 risk mitigation actions is **7.911**
- Total exposure (deterministic exposure) per man-hour released by not performing 51 risk mitigation actions is **1.708**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 51 risk mitigation actions is **4.777**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 51 risk mitigation actions is **1.332**

If **Policy 12** is applied, as we see in Table 29

- Risk Mitigation Actions shall be performed for **20** of 102 risk items. Risks with # '73', '1', '94', '55', '69', '29', '82', '57', '95', '97', '49', '62', '93', '70', '4', '56', '100', '101', '23', and '92' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **82** of 102 risk items. Risks with # '64', '96', '74', '91', '75', '72', '84', '89', '58', '60', '50', '86', '10', '15', '77', '87', '98', '20', '25', '13', '61', '3', '99', '68', '2', '54', '21', '63', '76', '46', '45', '88', '28', '53', '59', '33', '14', '65', '90', '80', '102', '12', '44', '85', '51', '26', '8', '24', '5', '36', '67', '16', '22', '32', '37', '39', '47', '43', '48', '34', '6', '9', '66', '38', '19', '17', '30', '41', '52', '7', '71', '83', '35', '79', '31', '27', '78', '18', '42', '11', '81', and '40' shall be monitored.
- Risk Mitigation Costs are **331 man-hours** for these 20 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **5064 man-hours** for these monitored 82 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 20 risk mitigation actions is **4.812**
- Total exposure (deterministic exposure) per man-hour released by not performing 82 risk mitigation actions is **4.807**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 20 risk mitigation actions is **2.827**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 82 risk mitigation actions is **3.281**

4.3.3 Policy 13-18

"Product Engineering" Class:

There are 42 risk items in this class. According to Risk Prioritization Method 3, the prioritization of these 42 risk items can be seen in Table 30 at Appendix C.

After three different threshold calculation methods applied to the risks within "Product Engineering" class (Table 30), the values for threshold levels are;

Threshold 1 = **0.039** (the average of the "exposure * probability for mitigation / risk mitigation cost" values in Table 30)

Threshold 2 = **0.027** (the median of the "exposure * probability for mitigation / risk mitigation cost" values in Table 30)

Threshold 3 = **0.053** (the pareto principle point of the "exposure * probability for mitigation / risk mitigation cost" values in Table 30)

In Figure 11 at Appendix D, there is the distribution of "exposure * probability for mitigation / risk mitigation cost" values of the risks within "Product Enginieering" class, sorted in accordance with Risk Prioritization Method 3.

If **Policy 13** is applied, as we see in Table 30

- Risk Mitigation Actions shall be performed for **16** of 42 risk items. Risks with # '1', '10', '4', '23', '29', '15', '25', '3', '2', '28', '13', '20', '14', '21', '12' and '33' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **26** of 42 risk items. Risks with # '8', '36', '22', '32', '5', '16', '26', '6', '37', '39', '24', '17', '34', '19', '35', '38', '7', '9', '30', '31', '27', '41', '18', '42', '11', and '40' shall be monitored.
- Risk Mitigation Costs are **536 man-hours** for these 16 mitigated risk items.
- Risk Mitigation Costs would be **2168 man-hours** for these monitored 26 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 16 risk mitigation actions is **1.873**
- Total exposure (deterministic exposure) per man-hour released by not performing 26 risk mitigation actions is **0.725**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 16 risk mitigation actions is **1.086**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 26 risk mitigation actions is **0.537**

If **Policy 14** is applied, as we see in Table 30

- Risk Mitigation Actions shall be performed for **21** of 42 risk items. Risks with # '1', '10', '4', '23', '29', '15', '25', '3', '2', '28', '13', '20', '14', '21', '12', '33', '8', '36', '22', '32', and '5' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **21** of 42 risk items. Risks with # '16', '26', '6', '37', '39', '24', '17', '34', '19', '35', '38', '7', '9', '30', '31', '27', '41', '18', '42', '11', and '40' shall be monitored.
- Risk Mitigation Costs are **924 man-hours** for these 21 mitigated risk items.
- Risk Mitigation Costs would be **1780 man-hours** for these monitored 21 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 21 risk mitigation actions is **2.065**
- Total exposure (deterministic exposure) per man-hour released by not performing 21 risk mitigation actions is **0.533**

- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 21 risk mitigation actions is **1.240**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 21 risk mitigation actions is **0.384**

If **Policy 15** is applied, as we see in Table 30

- Risk Mitigation Actions shall be performed for **8** of 42 risk items. Risks with # '1', '10', '4', '23', '29', '15', '25', and '3' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **34** of 42 risk items. Risks with # '2', '28', '13', '20', '14', '21', '12', '33', '8', '36', '22', and '32' '5', '16', '26', '6', '37', '39', '24', '17', '34', '19', '35', '38', '7', '9', '30', '31', '27', '41', '18', '42', '11', and '40' shall be monitored.
- Risk Mitigation Costs are **232 man-hours** for these 8 mitigated risk items.
- Risk Mitigation Costs would be **2472 man-hours** for these monitored 34 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 8 risk mitigation actions is **1.344**
- Total exposure (deterministic exposure) per man-hour released by not performing 34 risk mitigation actions is **1.253**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 8 risk mitigation actions is **0.715**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 34 risk mitigation actions is **0.909**

"Development Environment" Class:

There are 29 risk items in this class. According to Risk Prioritization Method 3, the prioritization of these 29 risk items can be seen in Table 31 at Appendix C.

After three different threshold calculation methods applied to the risks within "Development Environment" class (Table 31), the values for threshold levels are;

Threshold 1 = **0.072** (the average of the "exposure * probability for mitigation / risk mitigation cost" values in Table 31)

Threshold 2 = **0.050** (the median of the "exposure * probability for mitigation / risk mitigation cost" values in Table 31)

Threshold 3 = **0.109** (the pareto principle point of the "exposure * probability for mitigation / risk mitigation cost" values in Table 31)

In Figure 12 at Appendix D, there is the distribution of "exposure * probability for mitigation / risk mitigation cost" values of the risks within "Development Environment" class, sorted in accordance with Risk Prioritization Method 3.

If **Policy 13** is applied, as we see in Table 31

- Risk Mitigation Actions shall be performed for **10** of 29 risk items. Risks with # ‘55’, ‘69’, ‘70’, ‘57’, ‘49’, ‘62’, ‘58’, ‘60’, ‘56’, and ‘64’ shall be mitigated.
- Risk Mitigation Actions shall not be performed for **19** of 29 risk items. Risks with # ‘68’, ‘50’, ‘45’, ‘54’, ‘46’, ‘63’, ‘59’, ‘61’, ‘51’, ‘44’, ‘65’, ‘67’, ‘53’, ‘47’, ‘43’, ‘48’, ‘66’, ‘71’, and ‘52’ shall be monitored.
- Risk Mitigation Costs are **215 man-hours** for these 10 mitigated risk items. (After converting of YTL to man-hour by ‘1 man-hour = 15 YTL’)
- Risk Mitigation Costs would be **1012 man-hours** for these monitored 19 risk items.
- Total exposure (deterministic exposure) per man-hour prevented by performing 10 risk mitigation actions is **2.015**
- Total exposure (deterministic exposure) per man-hour released by not performing 19 risk mitigation actions is **0.987**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 10 risk mitigation actions is **1.356**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 19 risk mitigation actions is **0.734**

If **Policy 14** is applied, as we see in Table 31

- Risk Mitigation Actions shall be performed for **15** of 29 risk items. Risks with # ‘55’, ‘69’, ‘70’, ‘57’, ‘49’, ‘62’, ‘58’, ‘60’, ‘56’, ‘64’, ‘68’, ‘50’, ‘45’, ‘54’, and ‘46’ shall be mitigated.
- Risk Mitigation Actions shall not be performed for **14** of 29 risk items. Risks with # ‘63’, ‘59’, ‘61’, ‘51’, ‘44’, ‘65’, ‘67’, ‘53’, ‘47’, ‘43’, ‘48’, ‘66’, ‘71’, and ‘52’ shall be monitored.
- Risk Mitigation Costs are **359 man-hours** for these 15 mitigated risk items. (After converting of YTL to man-hour by ‘1 man-hour = 15 YTL’)
- Risk Mitigation Costs would be **868 man-hours** for these monitored 14 risk items.
- Total exposure (deterministic exposure) per man-hour prevented by performing 15 risk mitigation actions is **2.398**
- Total exposure (deterministic exposure) per man-hour released by not performing 14 risk mitigation actions is **0.605**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 15 risk mitigation actions is **1.627**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 14 risk mitigation actions is **0.463**

If **Policy 15** is applied, as we see in Table 31

- Risk Mitigation Actions shall be performed for **6** of 29 risk items. Risks with # ‘55’, ‘69’, ‘70’, ‘57’, ‘49’, and ‘62’ shall be mitigated.
- Risk Mitigation Actions shall not be performed for **23** of 29 risk items. Risks with # ‘58’, ‘60’, ‘56’, ‘64’, ‘68’, ‘50’, ‘45’, ‘54’, ‘46’, ‘63’, ‘59’, ‘61’, ‘51’, ‘44’, ‘65’, ‘67’, ‘53’, ‘47’, ‘43’, ‘48’, ‘66’, ‘71’, and ‘52’ shall be monitored.

- Risk Mitigation Costs are **103 man-hours** for these 6 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **1124 man-hours** for these monitored 23 risk items.
- Total exposure (deterministic exposure) per man-hour prevented by performing 6 risk mitigation actions is **1.426**
- Total exposure (deterministic exposure) per man-hour released by not performing 23 risk mitigation actions is **1.576**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 6 risk mitigation actions is **0.988**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 23 risk mitigation actions is **1.102**

"Program Constraints" Class:

There are 31 risk items in this class. According to Risk Prioritization Method 3, the prioritization of these 31 risk items can be seen in Table 32 at Appendix C.

After three different threshold calculation methods applied to the risks within "Program Constraints" class (Table 32), the values for threshold levels are;

Threshold 1 = **0.080** (the average of the "exposure * probability for mitigation / risk mitigation cost" values in Table 32)

Threshold 2 = **0.063** (the median of the "exposure * probability for mitigation / risk mitigation cost" values in Table 32)

Threshold 3 = **0.109** (the pareto principle point of the "exposure * probability for mitigation / risk mitigation cost" values in Table 32)

In Figure 13 at Appendix D, there is the distribution of "exposure * probability for mitigation / risk mitigation cost"values of the risks within "Program Constraints" class, sorted in accordance with Risk Prioritization Method 3.

If **Policy 13** is applied, as we see in Table 32

- Risk Mitigation Actions shall be performed for **11** of 31 risk items. Risks with # '73', '82', '94', '77', '72', '95', '97', '93', '101', '92', and '100' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **20** of 31 risk items. Risks with # '96', '87', '86', '91', '84', '89', '74', '75', '98', '80', '99', '90', '76', '85', '88', '102', '79', '78', '83', and '81' shall be monitored.
- Risk Mitigation Costs are **192 man-hours** for these 11 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')

- Risk Mitigation Costs would be **1272 man-hours** for these monitored 20 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 11 risk mitigation actions is **2.453**
- Total exposure (deterministic exposure) per man-hour released by not performing 20 risk mitigation actions is **1.566**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 11 risk mitigation actions is **1.591**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 20 risk mitigation actions is **0.888**

If **Policy 14** is applied, as we see in Table 32

- Risk Mitigation Actions shall be performed for **17** of 31 risk items. Risks with # '73', '82', '94', '77', '72', '95', '97', '93', '101', '92', '100', '96', '87', '86', '91', '84', and '89' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **14** of 31 risk items. Risks with # '74', '75', '98', '80', '99', '90', '76', '85', '88', '102', '79', '78', '83', and '81' shall be monitored.
- Risk Mitigation Costs are **332 man-hours** for these 17 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **1132 man-hours** for these monitored 14 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 17 risk mitigation actions is **3.196**
- Total exposure (deterministic exposure) per man-hour released by not performing 14 risk mitigation actions is **0.823**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 17 risk mitigation actions is **1.994**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 14 risk mitigation actions is **0.485**

If **Policy 15** is applied, as we see in Table 32

- Risk Mitigation Actions shall be performed for **8** of 31 risk items. Risks with # '73', '82', '94', '77', '72', '95', '97', and '93'shall be mitigated.
- Risk Mitigation Actions shall not be performed for **23** of 31 risk items. Risks with # '101', '92', '100', '96', '87', '86', '91', '84', '89', '74', '75', '98', '80', '99', '90', '76', '85', '88', '102', '79', '78', '83', and '81' shall be monitored.
- Risk Mitigation Costs are **120 man-hours** for these 8 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **1344 man-hours** for these monitored 23 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 8 risk mitigation actions is **1.924**
- Total exposure (deterministic exposure) per man-hour released by not performing 23 risk mitigation actions is **2.095**

- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 8 risk mitigation actions is **1.292**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 23 risk mitigation actions is **1.187**

"Whole Set of Risks":

There are 102 risk items in the whole set. According to Risk Prioritization Method 3, the prioritization of these 102 risk items can be seen in Table 33 at Appendix C.

After three different threshold calculation methods applied to the whole set of risks (Table 33), the values for threshold levels are;

Threshold 1 = **0.060** (the average of the "exposure * probability for mitigation / risk mitigation cost" values in Table 33)

Threshold 2 = **0.045** (the median of the "exposure * probability for mitigation / risk mitigation cost" values in Table 33)

Threshold 3 = **0.094** (the pareto principle point of the "exposure * probability for mitigation / risk mitigation cost" values in Table 33)

In Figure 14 at Appendix D, there is the distribution of "exposure * probability for mitigation / risk mitigation cost" values of the whole set of risks, sorted in accordance with Risk Prioritization Method 3.

If **Policy 16** is applied, as we see in Table 33

- Risk Mitigation Actions shall be performed for **34** of 102 risk items. Risks with # '73', '55', '69', '82', '1', '94', '70', '57', '49', '72', '95', '97', '62', '93', '101', '92', '58', '60', '10', '4', '56', '100', '23', '77', '29', '64', '96', '15', '87', '91', '86', '84', '89', and '68' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **68** of 102 risk items. Risks with # '25', '74', '50', '45', '3', '2', '54', '28', '75', '13', '46', '63', '59', '98', '20', '61', '99', '14', '80', '21', '12', '33', '90', '51', '76', '44', '8', '85', '88', '65', '102', '67', '53', '47', '36', '22', '32', '43', '5', '16', '26', '48', '6', '37', '39', '24', '66', '17', '34', '71', '19', '35', '38', '7', '79', '9', '30', '78', '31', '27', '83', '41', '52', '18', '42', '11', '81', and '40' shall be monitored.
- Risk Mitigation Costs are **691 man-hours** for these 34 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **4704 man-hours** for these monitored 68 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 34 risk mitigation actions is **6.471**

- Total exposure (deterministic exposure) per man-hour released by not performing 68 risk mitigation actions is **3.148**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 34 risk mitigation actions is **3.929**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 68 risk mitigation actions is **2.180**

If **Policy 17** is applied, as we see in Table 33

- Risk Mitigation Actions shall be performed for **53** of 102 risk items. Risks with # '73', '55', '69', '82', '1', '94', '70', '57', '49', '72', '95', '97', '62', '93', '101', '92', '58', '60', '10', '4', '56', '100', '23', '77', '29', '64', '96', '15', '87', '91', '86', '84', '89', '68', '25', '74', '50', '45', '3', '2', '54', '28', '75', '13', '46', '63', '59', '98', '20', '61', '99', '14', and '80' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **49** of 102 risk items. Risks with # '21', '12', '33', '90', '51', '76', '44', '8', '85', '88', '65', '102', '67', '53', '47', '36', '22', '32', '43', '5', '16', '26', '48', '6', '37', '39', '24', '66', '17', '34', '71', '19', '35', '38', '7', '79', '9', '30', '78', '31', '27', '83', '41', '52', '18', '42', '11', '81', and '40' shall be monitored.
- Risk Mitigation Costs are **1387 man-hours** for these 53 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **4008 man-hours** for these monitored 49 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Total exposure (deterministic exposure) per man-hour prevented by performing 53 risk mitigation actions is **7.985**
- Total exposure (deterministic exposure) per man-hour released by not performing 49 risk mitigation actions is **1.634**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 53 risk mitigation actions is **4.884**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 49 risk mitigation actions is **1.225**

If **Policy 18** is applied, as we see in Table 33

- Risk Mitigation Actions shall be performed for **22** of 102 risk items. Risks with # '73', '55', '69', '82', '1', '94', '70', '57', '49', '72', '95', '97', '62', '93', '101', '92', '58', '60', '10', '4', '56', and '100' shall be mitigated.
- Risk Mitigation Actions shall not be performed for **80** of 102 risk items. Risks with # '23', '77', '29', '64', '96', '15', '87', '91', '86', '84', '89', '68', '25', '74', '50', '45', '3', '2', '54', '28', '75', '13', '46', '63', '59', '98', '20', '61', '99', '14', '80', '21', '12', '33', '90', '51', '76', '44', '8', '85', '88', '65', '102', '67', '53', '47', '36', '22', '32', '43', '5', '16', '26', '48', '6', '37', '39', '24', '66', '17', '34', '71', '19', '35', '38', '7', '79', '9', '30', '78', '31', '27', '83', '41', '52', '18', '42', '11', '81', and '40' shall be monitored.
- Risk Mitigation Costs are **443 man-hours** for these 22 mitigated risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')
- Risk Mitigation Costs would be **4952 man-hours** for these monitored 80 risk items. (After converting of YTL to man-hour by '1 man-hour = 15 YTL')

- Total exposure (deterministic exposure) per man-hour prevented by performing 22 risk mitigation actions is **4.849**
- Total exposure (deterministic exposure) per man-hour released by not performing 80 risk mitigation actions is **4.770**
- Total expected exposure (probabilistic exposure) per man-hour prevented by performing 22 risk mitigation actions is **3.064**
- Total expected exposure (probabilistic exposure) per man-hour released by not performing 80 risk mitigation actions is **3.044**

4.4. Results of Application of Policies

Policies apply to each class of risks, and to the whole set of risks as defined in Section 4.3. To calculate the results for whole set of risks, the results for the each class of risk items should be added to each other per each decision parameter defined in Section 4.3.

The values of the decision parameters (defined in Section 4.2) for the defined policies (given in Section 4.1) are given in Tables 34-42 at Appendix E.

Tables 34-42 also show the building process of the values. Summary tables are needed to focus only on the results, not building process. Tables 17, 18, and 19 are the summary tables of the results.

Table 17 Values of Decision Parameters for Policy 1-6

	Policy 1	**Policy 2**	**Policy 3**	**Policy 4**	**Policy 5**	**Policy 6**
# of risk items mitigated	47	53	21	46	54	21
# of risk items monitored	55	49	81	56	48	81
percentage of risk items mitigated	0.46	0.52	0.21	0.45	0.53	0.21
total exposure prevented for mitigated risks	5.719	6.227	2.882	5.786	6.437	2.882
total exposure released for monitored risks	3.900	3.392	6.737	3.833	3.182	6.737
percentage of total exposure prevented	0.59	0.65	0.30	0.60	0.67	0.30
risk mitigation costs for mitigated risks (man-hour)	3105	3481	1399	2989	3357	1399
potential risk mitigation costs for monitored risks (man-hour)	2289	1913	3996	2425	2057	3996
percentage of risk mitigation costs	0.58	0.65	0.26	0.55	0.62	0.26
total expected exposure prevented for mitigated risks	3.588	3.867	2.078	3.596	3.967	1.994
total expected exposure released for monitored risks	2.520	2.241	4.114	2.512	2.141	4.114
percentage of total expected exposure prevented	0.59	0.63	0.34	0.59	0.65	0.33

Table 17 Values of Decision Parameters for Policy 1-6 (cont'd)

total exposure prevented for mitigated risks / # of risk items mitigated	0.122	0.117	0.137	0.126	0.119	0.137
risk mitigation costs for mitigated risks / # of risk items mitigated	66.06	65.68	66.62	64.98	62.17	66.62
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.076	0.073	0.099	0.078	0.073	0.095
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$18.42 * 10^{-4}$	$17.89 * 10^{-4}$	$20.60 * 10^{-4}$	$19.35 * 10^{-4}$	$19.17 * 10^{-4}$	$20.60 * 10^{-4}$
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$11.56 * 10^{-4}$	$11.11 * 10^{-4}$	$14.85 * 10^{-4}$	$12.03 * 10^{-4}$	$11.82 * 10^{-4}$	$14.25 * 10^{-4}$

Table 18 Values of Decision Parameters for Policy 7-12

	Policy 7	**Policy 8**	**Policy 9**	**Policy 10**	**Policy 11**	**Policy 12**
# of risk items mitigated	35	54	20	38	51	20
# of risk items monitored	67	48	82	64	51	82
percentage of risk items mitigated	0.34	0.53	0.20	0.37	0.50	0.20
total exposure prevented for mitigated risks	6.445	7.721	4.483	6.966	7.911	4.812
total exposure released for monitored risks	3.174	1.899	5.136	2.652	1.708	4.807
percentage of total exposure prevented	0.67	0.80	0.47	0.72	0.82	0.50
risk mitigation costs for mitigated risks (man-hour)	811	1611	403	779	1259	331
potential risk mitigation costs for monitored risks (man-hour)	4584	3784	4992	4616	4136	5064
percentage of risk mitigation costs	0.15	0.30	0.07	0.14	0.23	0.06
total expected exposure prevented for mitigated risks	3.828	4.701	2.709	4.127	4.777	2.827
total expected exposure released for monitored risks	2.281	1.407	3.484	1.982	1.332	3.281
percentage of total expected exposure prevented	0.63	0.77	0.44	0.68	0.78	0.46

Table 18 Values of Decision Parameters for Policy 7-12 (cont'd)

total exposure prevented for mitigated risks / # of risk items mitigated	0.184	0.143	0.224	0.183	0.155	0.241
risk mitigation costs for mitigated risks / # of risk items mitigated	23.17	29.83	20.15	20.50	24.69	16.55
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.109	0.087	0.135	0.109	0.094	0.141
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$79.47 * 10^{-4}$	$47.93 * 10^{-4}$	$111.24 * 10^{-4}$	$89.42 * 10^{-4}$	$62.84 * 10^{-4}$	$145.38 * 10^{-4}$
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$47.20 * 10^{-4}$	$29.18 * 10^{-4}$	$67.22 * 10^{-4}$	$52.98 * 10^{-4}$	$37.94 * 10^{-4}$	$85.41 * 10^{-4}$

Table 19 Values of Decision Parameters for Policy 13-18

	Policy 13	**Policy 14**	**Policy 15**	**Policy 16**	**Policy 17**	**Policy 18**
# of risk items mitigated	37	53	22	34	53	22
# of risk items monitored	65	49	80	68	49	80
percentage of risk items mitigated	0.36	0.52	0.22	0.33	0.52	0.22
total exposure prevented for mitigated risks	6.341	7.659	4.694	6.471	7.985	4.849
total exposure released for monitored risks	3.278	1.961	4.924	3.148	1.634	4.770
percentage of total exposure prevented	0.66	0.80	0.49	0.67	0.83	0.50
risk mitigation costs for mitigated risks (man-hour)	943	1615	455	691	1387	443
potential risk mitigation costs for monitored risks (man-hour)	4452	3780	4940	4704	4008	4952
percentage of risk mitigation costs	0.17	0.30	0.08	0.13	0.26	0.08
total expected exposure prevented for mitigated risks	4.033	4.861	2.995	3.929	4.884	3.064
total expected exposure released for monitored risks	2.159	1.332	3.198	2.180	1.225	3.044

Table 19 Values of Decision Parameters for Policy 13-18 (cont'd)

percentage of total expected exposure prevented	0.65	0.78	0.48	0.64	0.80	0.50
total exposure prevented for mitigated risks / # of risk items mitigated	0.171	0.145	0.213	0.190	0.151	0.220
risk mitigation costs for mitigated risks / # of risk items mitigated	25.49	30.47	20.68	20.32	26.17	20.14
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.109	0.092	0.136	0.116	0.092	0.139
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$67.24 * 10^{-4}$	$47.42 * 10^{-4}$	$103.16 * 10^{-4}$	$93.65 * 10^{-4}$	$57.57 * 10^{-4}$	$109.46 * 10^{-4}$
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$42.77 * 10^{-4}$	$30.10 * 10^{-4}$	$65.82 * 10^{-4}$	$56.86 * 10^{-4}$	$35.21 * 10^{-4}$	$69.16 * 10^{-4}$

4.5. Evaluating the Policies

As mentioned before, four main subjects that are designated in this study for evaluation purposes are risk items mitigated, exposures prevented, costs, and expected exposures prevented.

These four main subjects have been enlarged to decision parameters consisting of based decision parameters and derived decision parameters defined in Section 4.2.

Each preference profile defined in Section 4.2 highlights a characteristic of any decision parameter.

There is the data set of 102 risk items. On the base of this data set, the ranking of each policy in the context of each preference profile is given in Table 20. In this table, a rank of 1 corresponds to the policy to provide the best value for the related profile's decision parameter; and a rank of 18 corresponds to the policy to provide the worst value for the related profile's decision parameter.

Table 20 Ranks of Policies for Each Preference Profile

Profile	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Policy															
1	7	12	7	12	12	12	16	16	11	11	16	16	16	17	17
2	3	14	3	14	10	10	18	18	9	9	18	15	17	18	18
3	15	3	15	3	17	17	11	11	17	17	13	17	9	13	13
4	8	11	8	11	11	11	15	15	12	12	15	14	15	15	15
5	1	17	1	17	8	8	17	17	6	6	17	13	18	16	16
6	16	4	16	4	18	18	12	12	18	18	14	18	10	14	14
7	11	8	11	8	7	7	7	7	10	10	6	7	6	7	7
8	2	18	2	18	3	3	13	13	4	4	12	11	14	11	12
9	17	1	17	1	16	16	2	2	16	16	2	3	4	2	3
10	9	10	9	10	5	5	6	6	5	5	7	5	7	6	6
11	6	13	6	13	2	2	9	9	2	2	9	8	11	9	9
12	18	2	18	2	14	14	1	1	15	15	1	1	1	1	1
13	10	9	10	9	9	9	8	8	7	7	8	9	8	8	8
14	4	14	4	14	4	4	14	14	3	3	11	12	12	12	11
15	13	5	13	5	15	15	4	4	14	14	4	6	3	4	4
16	12	7	12	7	6	6	5	5	8	8	5	4	5	5	5
17	5	14	5	14	1	1	10	10	1	1	10	10	13	10	10
18	14	6	14	6	13	13	3	3	13	13	3	2	2	3	2

4.6. Analyzing the Results Regarding Suitable Policies for Different Preference Profiles

Main evaluation parameters in this study are risk items mitigated, exposures prevented, costs, and expected exposures prevented as mentioned before. As the values in Table 20 are analyzed, it is seen that some profiles have the same policy rankings. These are

- Profile 1 & 3
- Profile 2 & 4
- Profile 5 & 6
- Profile 7 & 8
- Profile 9 & 10

Profile 1 & 3 are related with risk items mitigated. In the data set, there are 102 risk items. However, # of risk items mitigated changes according to applied policy. Profile 1 seeks for maximum of # of risk items mitigated. Profile 3 seeks for maximum of percentage of risk items mitigated. Because of the data set having fix items of risk items for all policies, the ranking of policies for Profile 1 is the same as the ranking of policies for Profile 3.

Profile 2 & 4 are also related with risk items mitigated. In the data set, there are 102 risk items. However, # of risk items mitigated changes according to applied policy. Profile 2 seeks for minimum of # of risk items mitigated. Profile 4 seeks for minimum of percentage of risk items mitigated. Because of the data set having fix items of risk items for all policies, the ranking of policies for Profile 2 is the same as the ranking of policies for Profile 4.

Profile 5 & 6 are related with exposures prevented. Total exposure for all of the risks in the data set is a certain value and is never changing. Profile 5 seeks for maximum of total exposure prevented for mitigated risks. Profile 6 seeks for maximum of percentage of total exposure prevented. Because of the total exposure value of all the risk items in the data set being fix, the ranking of policies for Profile 5 is the same as the ranking of policies for Profile 6.

Profile 7 & 8 are related with mitigation costs. Total mitigation cost for all of the risks in the data set is a certain value and is never changing. Profile 7 seeks for minimum of risk mitigation costs for mitigated risks. Profile 8 seeks for minimum of percentage of risk mitigation costs. Because of the total mitigation cost value of all the risk items in the data set being fix, the ranking of policies for Profile 7 is the same as the ranking of policies for Profile 8.

Profile 9 & 10 are related with expected exposures prevented. Total expected exposure for all of the risks in the data set is a certain value and is never changing. Profile 9 seeks for maximum of total expected exposure prevented for mitigated risks. Profile 10 seeks for maximum of percentage of total expected exposure prevented. Because of the total expected exposure value of all the risk items in the data set being fix, the ranking of policies for Profile 9 is the same as the ranking of policies for Profile 10.

Profiles in Table 20 have some similarities as mentioned above. It is wise to combine the profiles into one to represent profile groups. Combination of the profiles is shown in Table 21, as revising of Table 20. Therefore, 10 profile entities remain for further consideration.

Table 21 Ranks of Policies for Each Revised Profile Set

Profile	1&3	2&4	5&6	7&8	9&10	11	12	13	14	15	Sum of Ranks
Policy											
1	7	12	12	16	11	16	16	16	17	17	140
2	3	14	10	18	9	18	15	17	18	18	140
3	15	3	17	11	17	13	17	9	13	13	128
4	8	11	11	15	12	15	14	15	15	15	131
5	1	17	8	17	6	17	13	18	16	16	129
6	16	4	18	12	18	14	18	10	14	14	138
7	11	8	7	7	10	6	7	6	7	7	76
8	2	18	3	13	4	12	11	14	11	12	100
9	17	1	16	2	16	2	3	4	2	3	66
10	9	10	5	6	5	7	5	7	6	6	66
11	6	13	2	9	2	9	8	11	9	9	78
12	18	2	14	1	15	1	1	1	1	1	55
13	10	9	9	8	7	8	9	8	8	8	84
14	4	14	4	14	3	11	12	12	12	11	97
15	13	5	15	4	14	4	6	3	4	4	72
16	12	7	6	5	8	5	4	5	5	5	62
17	5	14	1	10	1	10	10	13	10	10	84
18	14	6	13	3	13	3	2	2	3	2	61

Policy 5 is the most suitable one for Profile 1&3; Policy 9 is the most suitable one for Profile 2&4. If having look at the elements of Policy 5 and Policy 9, seen that there is no same element for Risk Prioritization Method, Application set, and Threshold definition for Policy 5 and 9. It is expected, because the aims of Profile 1&3 and Profile 2&4 are completely opposite.

Policy 17 is the most suitable one for Profile 5&6 and Profile 9&10. Both profile sets are similar since total expected exposure values are calculated by total exposure

values multiplied by probability for mitigation values. Profile 5&6 is related with total exposure, Profile 9&10 is related with total expected exposure.

Policy 12 is the most suitable one for Profile 7&8. Threshold definition in Policy 12 is threshold 3. Threshold 3 among three threshold definitions leads to relatively less number of risk items mitigated. Therefore, risk mitigation costs are less than the other threshold definitions.

Policy 12 is also the most suitable one for Profile 11, 12, 13, 14 and 15. Threshold definition in Policy 12 is threshold 3. Threshold 3 puts less number of risk items mitigated than the other thresholds. These risk items determined by threshold 3 has the more exposure values, and less risk mitigation costs compared to the risk items determined by the other thresholds. Therefore, Policy 12 is the most suitable one for these profiles.

If each of the 10 profile set weighted equally in Table 21, a policy's rank summation through 10 profiles is put forward as an indicator which shows the policy's overall performance. Policy 12 is the most suitable policy since its 'sum of ranks' value is the lowest.

CHAPTER 5

CONCLUSION

Risk management is an effective tool that prevents the organization to deviate from its objectives. Risk management can be either quantifying or qualitative. Qualitative risk management is based on the personnel's subjective ideas, but quantifying risk management is based on the numerical parameters. In the literature, there are sources for risk management. Some of them are qualitative, and some of them are quantitative. However, there is no much source about the application study of a quantifying risk management process on a software organization. Hence, this study has aimed to address this niche by following the method described extensively in subsequent paragraphs and sections.

Risk management can be applied to all kinds of business areas. If the business area is software organization, there are helpful sources in the literature for risk management. One of these is Risk Taxonomy classification published by Software Engineering Institute (SEI).

During the phase of risk identification and risk classification, Risk Taxonomy has been used in this study. Risk probability and impact values are estimated for the identified risks. Risk exposure values are calculated by using risk probability and impact values. Risk mitigation actions are defined, and their costs are calculated for each risk item. Then, probabilities for mitigation values are estimated. We need to sort the risk items, and define a threshold value to separate mitigated risk items from monitored risk items. For this reason, risk prioritization methods are built, and threshold definitions are defined.

Quantifying risk management policies are based on three parameters. Risk prioritization methods, threshold definitions, and application set. By all combination of these parameters, 18 (=3*3*2) policies have been formed. In the other side, preference profiles based on decision parameters have been formed. Policies have been applied to the data set for the software organization. The results of the application of the policies have been analyzed in terms of decision parameters. Therefore, policies have been evaluated and ranked for each preference profile.

An organization, working in the software development business, can benefit from this study for quantifying risk management as followings:

- The organization can assume the data in this study as universally accepted, because it includes risk taxonomy conduction, so directly uses the results in Table 21. The organization chooses the preference profile for itself from Table 16, gets the most suitable policy from Table 21 for the related profile, and applies this policy as defined in Table 15 for quantifying risk management.
- The organization can conduct this study by its own data. So, the results in Table 21 changes for the organization. The organization chooses the preference profile for itself from Table 16, gets the most suitable policy from changed Table 21 for the related profile, and applies this policy as defined in Table 15 for quantifying risk management.

The content of this study shows conformity to CMMI Level-3 and ISO 9001:2000

- **CMMI (Capability Maturity Model for Integration):** [27]

  SP 1.1 Determine Risk Sources and Categories

  Met by ‘Risk Identification’ and ‘Risk Classification’ paragraphs.

  SP 1.2 Define Risk Parameters

  Met by ‘Risk Probability’, ‘Risk Impact’ and ‘Risk Exposure’ paragraphs.

SP 1.3 Establish a Risk Management Strategy

Met by ‘Thresholds’ paragraph.

SP 2.1 Identify Risks

Met by ‘Risk Identification’ paragraph.

SP 2.2 Evaluate, Categorize, and Prioritize Risks

Met by ‘Risk Classification’, ‘Risk Probability’, ‘Risk Impact’, ‘Risk Exposure’ and ‘Risk Prioritization’ paragraphs.

SP 3.1 Develop Risk Mitigation Plans

Met by ‘Risk Mitigation Action’ and ‘Risk Mitigation Cost’ paragraphs.

SP 3.2 Implement Risk Mitigation Plans

Met by ‘Risk Mitigation Action’ and ‘Risk Mitigation Cost’ paragraphs.

- **ISO (International Organization for Standardization) 9001:2000**:

  This International Standard does not include requirements specific to other management systems, such as those particular to environmental management, occupational health and safety management, financial management or risk management. However, this International Standard enables an organization to align or integrate its own quality management system with related management system requirements.

The following lists some areas that can be addressed by further studies about the same subject:

- The preference profiles related with risk items mitigated, total exposures covered, costs, and total expected exposures can be enlarged by requesting feedbacks from risk management stakeholders.
- The frequency of the risk occurrence can be used in calculation of “risk exposure”

- Formal “Decision Analysis and Resolution (DAR)” process can be used during choosing risk mitigation actions from the alternatives

REFERENCES

1 Aubert, B.A., Patry, M., and Rivard, S., "A Framework for Information Technology Outsourcing Risk Managemet", The DATA BASE for Advances in Information Systems, Vol.36 No.4, 2005, pp. 9-28.

2 Blakley, B., McDermott, E., and Geer, D., "Information Security is Information Risk Management", Cloudcroft, New Mexico, September 2002, pp. 97-104.

3 Boehm, B., "Software Risk Management: Principles and Practices", Defense Advanced Research Projects Agency, January 1991, pp. 32-41.

4 Carbone, T., and Tippett, D., "Project Risk Management Using the Project Risk FMEA", Engineering Management Journal, Vol.16 No.4, December 2004, pp. 28-35.

5 Chapman, C., "Project risk analysis and management – PRAM the generic process", International Journal of Project Management Vol.15 No.5, 1997, pp. 273-281.

6 Dedolph, F.M., "The Neglected Management Activity: Software Risk Management", Bell Labs Technical Journal, Lucent Technologies Inc., 2003, pp. 91-95.

7 Doherty, N.A., "Corporate Risk Management", McGraw-Hill Inc., 1985.

8 Elkington, P., and Smallman, C., "Managing project risks: a case study from the utilities sector", International Journal of Project Management 20, 2002, pp. 49-57.

9 Fairley, R.E., "Software Risk Management", IEEE Software, May/June 2005, pp. 101.

10 Grey, S., "Practical Risk Assessment for Project Management", John Wiley & Sons Ltd., 1995.

11 Hamdi, M., and Boudriga, N., “Algebraic Specification of Network Security Risk Management”, CNAS Research Lab., Telecommunication School of Engineering, October 2003, pp. 52-60.

12 Higuera, R.P., and Dorofee, A.J., “Team Risk Management: A New Model for Customer-Supplier Relationships”, CMU/SEI-94-SR-005, July 1994.

13 Keefer, G., “A CMMI Compatible Risk Management Process”, AVOCA GmbH, 2002.

14 Khan, F.I., and Haddara, M.M., “Risk-based maintenance (RBM): a quantitative approach for maintenance/inspection scheduling and planning”, Journal of Loss Prevention in the Process Industries Vol.16, 2003, pp. 561-573.

15 Kirkpatrick, R. J., Walker, J. A., and Firth, R., “Software Development Risk Management: An SEI Appraisal”, Software Engineering Institute, Carnegie Mellon University, 1992.

16 Kloman, H.F., “Risk Management Agonists” Risk Analysis 10, 1990, pp. 201-205.

17 Kwak, Y.H., and Stoddard, J., “Project risk management: lessons learned from software development environment”, Elsevier Science Ltd., 2003, pp. 915-920.

18 Levin, M., and Schneider, M., “Making the Distinction: Risk Management, Risk Exposure”, Risk Management, Vol.44 No.8, 1997, pp. 36-42.

19 Lowrance, W., “Acceptable Risk”, Los Altos, California, 1976.

20 Marvin, J.C., Suresh, L.K., and Ira, M., “Taxonomy-Based Risk Identification”, CMU/SEI-99-TR-009, June 1993.

21 Maude, T., and Willis, G., “Rapid Prototyping”, Pitman Publishing, 1991.

22 Patterson, F.D., and Nealiey, K., “A Risk Register Database System to aid the management of project risk”, International Journal of Project Management Vol.20, 2002, pp. 365-374.

23 Raz, T., and Michael, E., “Use and benefits of tools for project risk managemet”, International Journal of Project Management Vol.19, 2001, pp. 9-17.

24 Ronald, P.H., Yacov, Y.H., “Software Risk Management”, CMU/SEI-96-TR-012, June 1996.

25 Ropponen, J., and Lyytinen, K., “Components of Software Development Risk: How to Address Them”, IEEE Transactions on Software Engineering Vol.26, 2000, pp. 98-112.

26 Schmit, J.T., and Roth, K., “Cost Effectiveness of Risk Management Practices”, The Journal of Risk and Insurance, Vol. I.VII. No.3, 1990, pp. 455-470.

27 SEI (Softare Engineering Institute), “Capability Maturity Model® Integration Version 1.1”, March 2002.

28 Simon, P., and Hillson D., “Project Risk Analysis and Management (PRAM) guide”, UK: The Association for Project Management, 1997.

29 Ulrich, C., Walker, F., “Taxonomy-Based Risk Identification”, CMU/SEI-93-TR-6, June 1993.

30 Ward, S., “Requirements for an Effective Project Risk Management Process”, Project Management Journal, Vol.30 No.3, September 1999, pp. 37-43.

APPENDIX A

COMPLETE RISK TAXONOMY [29]

Taxonomy based risk identification approach describes a method for facilitating systematic and repeatable identification of risks associated with the development of a software dependent project. This method, derived from published literature and previous experience in developing software, was tested in active government-funded defence and civilian software development projects for both its usefulness and for improving the method itself.

The software taxonomy is organized into three major classes

1. **Product Engineering**: The technical aspects of the work to be accomplished.
2. **Development Environment**: The methods, procedures, and tools used to produce the product.
3. **Program Constraints**: The contractual, organizational, and operational factors within which the software is developed but which are generally outside of the direct control of the local management.

These taxonomic classes are further divided into elements and each element is characterized by its attributes.

1. Product Engineering Class

The product engineering class consists of the intellectual and physical activities required to build the product to be delivered to the customer. It includes the complete system hardware, software, and documentation. The class focuses on the work to be performed, and includes the following elements:

1.1. **Requirements**: The definition of what the software product is to do, the needs it must meet, how it is to behave, and how it will be used. This element also addresses the feasibility of developing the product and the scale of the effort.

1.1.1. **Stability**. The stability attribute refers to the degree to which the requirements are changing and the possible effect changing requirements and external interfaces will have on the quality, functionality, schedule, design, integration, and testing of the product being built. The attribute also includes issues that arise from the inability to control rapidly changing requirements.

For example, impact analyses may be inaccurate because it is impossible to define the baseline against which the changes will be implemented.

1.1.2. **Completeness.** Missing or incompletely specified requirements may appear in many forms, such as a requirements document with many functions or parameters "to be defined"; requirements that are not specified adequately to develop acceptance criteria, or inadvertently omitted requirements. When missing information is not supplied in a timely manner, implementation may be based on contractor assumptions that differ from customer expectations. When customer expectations are not documented in the specification, they are not budgeted into the cost and schedule.

1.1.3. **Clarity.** This attribute refers to ambiguously or imprecisely written individual requirements that are not resolved until late in the development phase. This lack of a mutual contractor and customer understanding may require re-work to meet the customer intent for a requirement.

1.1.4. **Validity.** This attribute refers to whether the aggregate requirements reflect customer intentions for the product. This may be affected by misunderstandings of the written requirements by the contractor or customer, unwritten customer expectations or requirements, or a specification in which the end user did not have inputs. This attribute is affected by the completeness and clarity attributes of the requirements specifications, but refers to the larger question of the system as a whole meeting customer intent.

1.1.5. **Feasibility.** The feasibility attribute refers to the difficulty of implementing a single technical or operational requirement, or of simultaneously meeting conflicting requirements. Sometimes two requirements by themselves are feasible, but together are not; they cannot both exist in the same product at the same time. Also included is the ability to determine an adequate qualification method for demonstration that the system satisfies the requirement.

1.1.6. **Precedent.** The precedent attribute concerns capabilities that have not been successfully implemented in any existing systems or are beyond the experience of program personnel or of the company. The degree of risk depends on allocation of additional schedule and budget to determine the feasibility of their implementation; contingency plans in case the requirements are not feasible as stated; and flexibility in the contract to allocate implementation budget and schedule based on the outcome of the feasibility study. Even when unprecedented requirements are feasible, there may still be a risk of underestimating the difficulty of implementation and committing to an inadequate budget and schedule.

1.1.7. **Scale.** This attribute covers both technical and management challenges presented by large complex systems development. Technical challenges include satisfaction of timing, scheduling and response requirements, communication among processors, complexity of system integration, analysis of inter-component dependencies, and impact due to changes in requirements. Management of a large number of tasks and people introduces a complexity in such areas as project organization, delegation of responsibilities, communication among management and peers, and configuration management.

1.2. **Design**: The translation of requirements into an effective design within project and operational constraints.

1.2.1. **Functionality**. This attribute covers functional requirements that may not submit to a feasible design, or use of specified algorithms or designs without a

high degree of certainty that they will satisfy their source requirements. Algorithm and design studies may not have used appropriate investigation techniques or may show marginal feasibility.

1.2.2. **Difficulty**. The difficulty attribute refers to functional or design requirements that may be extremely difficult to realize. Systems engineering may design a system architecture difficult to implement, or requirements analysis may have been based on optimistic design assumptions. The difficulty attribute differs from design feasibility in that it does not proceed from pre-ordained algorithms or designs.

1.2.3. **Interfaces**. This attribute covers all hardware and software interfaces that are within the scope of the development program, including interfaces between configuration items, and the techniques for defining and managing the interfaces. Special note is taken of non-developmental software and developmental hardware interfaces.

1.2.4. **Performance**. The performance attribute refers to time-critical performance: user and real-time response requirements, throughput requirements, performance analyses, and performance modelling throughout the development cycle.

1.2.5. **Testability**. The testability attribute covers the amenability of the design to testing, design of features to facilitate testing, and the inclusion in the design process of people who will design and conduct product tests.

1.2.6. **Hardware Constraints**. This attribute covers target hardware with respect to system and processor architecture, and the dependence on hardware to meet system and software performance requirements. These constraints may include throughput or memory speeds, real-time response capability, database access or capacity limitations, insufficient reliability, unsuitability to system function, or insufficiency in the amount of specified hardware.

1.2.7. **Non-Developmental Software**. Since non-developmental software (NDS) is not designed to system requirements, but selected as a "best fit," it may not conform precisely to performance, operability or supportability requirements. The customer may not accept vendor or developer test and reliability data to demonstrate satisfaction of the requirements allocated to NDS. It may then be difficult to produce this data to satisfy acceptance criteria and within the estimated NDS test budget. Requirements changes may necessitate re-engineering or reliance on vendors for special purpose upgrades.

1.3. **Code and Unit Test**: The translation of software designs into code that satisfies the requirements allocated to individual units.

1.3.1. **Feasibility**. The feasibility attribute of the code and unit test element addresses possible difficulties that may arise from poor design or design specification or from inherently difficult implementation needs.

1.3.2. **Unit Test**. Factors affecting unit test include planning and preparation and also the resources and time allocated for test.

1.3.3. **Coding/Implementation**. This attribute addresses the implications of implementation constraints. Some of these are: target hardware that is marginal or inadequate with regard to speed, architecture, memory size or external storage capacity; required implementation languages or methods; or differences between the development and target hardware.

1.4. **Integration and Test**: The integration of units into a working system and the validation that the software product performs as required.

1.4.1. **Environment**. The integration and test environment includes the hardware and software support facilities and adequate test cases reflecting realistic

operational scenarios and realistic test data and conditions. This attribute addresses the adequacy of this environment to enable integration in a realistic environment or to fully test all functional and performance requirements.

1.4.2. **Product.** The product integration attribute refers to integration of the software components to each other and to the target hardware, and testing of the contractually deliverable product. Factors that may affect this are internal interface specifications for hardware or software, testability of requirements, negotiation of customer agreement on test criteria, adequacy of test specifications, and sufficiency of time for integration and test.

1.4.3. **System**. The system integration attribute refers to integration of the contractual product to interfacing systems or sites. Factors associated with this attribute are external interface specifications, ability to faithfully produce system interface conditions prior to site or system integration, access to the system or site being interfaced to, adequacy of time for testing, and associate contractor relationships.

1.5. **Engineering Specialties**: Product requirements or development activities that may need specialized expertise such as safety, security, and reliability.

1.5.1. **Maintainability**. Maintainability may be impaired by poor software architecture, design, code, or documentation resulting from undefined or un-enforced standards, or from neglecting to analyze the system from a maintenance point of view.

1.5.2. **Reliability.** System reliability or availability requirements may be affected by hardware not meeting its reliability specifications or system complexity that aggravates difficulties in meeting recovery timelines. Reliability or availability requirements allocated to software may be stated in absolute terms, rather than as separable from hardware and independently testable.

1.5.3. **Safety**. This attribute addresses the difficulty of implementing allocated safety requirements and also the potential difficulty of demonstrating satisfaction of requirements by faithful simulation of the unsafe conditions and corrective actions. Full demonstration may not be possible until the system is installed and operational.

1.5.4. **Security**. This attribute addresses lack of experience in implementing the required level of system security that may result in underestimation of the effort required for rigorous verification methods, certification and accreditation, and secure or trusted development process logistics; developing to unprecedented requirements; and dependencies on delivery of certified hardware or software.

1.5.5. **Human Factors**. Meeting human factors requirements is dependent on understanding the operational environment of the installed system and agreement with various customer and user factions on a mutual understanding of the expectations embodied in the human factors requirements. It is difficult to convey this understanding in a written specification. Mutual agreement on the human interface may require continuous prototyping and demonstration to various customer factions.

1.5.6. **Specifications**. This attribute addresses specifications for the system, hardware, software, interface, or test requirements or design at any level with respect to feasibility of implementation and the quality attributes of stability, completeness, clarity, and verifiability.

2. Development Environment Class

The development environment class is concerned with the project environment in which a software product is engineered. This environment consists of the following elements:

2.1. **Development Process**: The definition, planning, documentation, suitability, enforcement, and communication of the methods and procedures used to develop the product.

2.1.1. **Formality**. Formality of the development process is a function of the degree to which a consistent process is defined, documented, and communicated for all aspects and phases of the development.

2.1.2. **Suitability.** Suitability refers to the adequacy with which the selected development model, process, methods, and tools support the scope and type of activities required for the specific program.

2.1.3. **Process Control**. Process control refers not only to ensuring usage of the defined process by program personnel, but also to the measurement and improvement of the process based on observation with respect to quality and productivity goals. Control may be complicated due to distributed development sites.

2.1.4. **Familiarity.** Familiarity with the development process covers knowledge of, experience in, and comfort with the prescribed process.

2.1.5. **Product Control**. Product control is dependent on traceability of requirements from the source specification through implementation such that the product test will demonstrate the source requirements. The change control process makes use of the traceability mechanism in impact analyses and reflects all resultant document modifications including interface and test documentation.

2.2. **Development System**: The tools and supporting equipment used in product development, such as computer-aided software engineering (CASE) tools, simulators, compilers, and host computer systems.

2.2.1. **Capacity**. Risks associated with the capacity of the development system may result from too few workstations, insufficient processing power or database storage, or other inadequacies in equipment to support parallel activities for development, test, and support activities.

2.2.2. **Suitability**. Suitability of the development system is associated with the degree to which it is supportive of the specific development models, processes, methods, procedures, and activities required and selected for the program. This includes the development, management, documentation, and configuration management processes.

2.2.3. **Usability.** Usability refers to development system documentation, accessibility and workspace, as well as ease of use.

2.2.4. **Familiarity**. Development system familiarity depends on prior use of the system by the company and by project personnel as well as adequate training for new users.

2.2.5. **Reliability.** Development system reliability is a measure of whether the needed components of the development system are available and working properly whenever required by any program personnel.

2.2.6. **System Support**. Development system support involves training in use of the system, access to expert users or consultants, and repair or resolution of problems by vendors.

2.2.7. **Deliverability**. Some contracts require delivery of the development system. Risks may result from neglecting to bid and allocate resources to ensure that the development system meets all deliverable requirements.

2.3. **Management Process**: The planning, monitoring, and controlling of budgets and schedules; controlling factors involved in defining, implementing, and testing the product; the project manager's experience in software development, management, and the product domain; and the manager's expertise in dealing with external organizations including customers, senior management, matrix management, and other contractors.

2.3.1. **Planning**. The planning attribute addresses risks associated with developing a well-defined plan that is responsive to contingencies as well as long-range goals and that was formulated with the input and acquiescence of those affected by it. Also addressed are managing according to the plan and formally modifying the plan when changes are necessary.

2.3.2. **Project Organization.** This attribute addresses the effectiveness of the program organization, the effective definition of roles and responsibilities, and the assurance that these roles and lines of authority are understood by program personnel.

2.3.3. **Management Experience**. This attribute refers to the experience of all levels of managers with respect to management, software development management, the application domain, the scale and complexity of the system and program, the selected development process, and hands-on development of software.

2.3.4. **Program Interfaces**. This attribute refers to the interactions of managers at all levels with program personnel at all levels, and with external personnel such as the customer, senior management, and peer managers.

2.4. **Management Methods**: The methods, tools, and supporting equipment that will be used to manage and control the product development, such as monitoring tools, personnel management, quality assurance, and configuration management.

2.4.1. **Monitoring**. The monitoring includes the activities of obtaining and acting upon status reports, allocating status information to the appropriate program organizations, and maintaining and using progress metrics.

2.4.2. **Personnel Management.** Personnel management refers to selection and training of program members and ensuring that they: take part in planning and customer interaction for their areas of responsibility; work according to plan; and receive the help they need or ask for to carry out their responsibilities.

2.4.3. **Quality Assurance**. The quality assurance attribute refers to the procedures instituted for ensuring both that contractual processes and standards are implemented properly for all program activities, and that the quality assurance function is adequately staffed to perform its duties.

2.4.4. **Configuration Management**. The configuration management (CM) attribute addresses both staffing and tools for the CM function as well as the complexity of the required CM process with respect to such factors as multiple development and installation sites and product coordination with existing, possibly changing, systems.

2.5. **Work Environment**: The general environment within which the work will be performed, including the attitudes of people and the levels of cooperation, communication, and morale.

2.5.1. **Quality Attitude**. This attribute refers to the tendency of program personnel to do quality work in general and to conform to specific quality standards for the program and product.

2.5.2. **Cooperation.** The cooperation attribute addresses lack of team spirit among development staff both within and across work groups and the failure of all management levels to demonstrate that best efforts are being made to remove barriers to efficient accomplishment of work.

2.5.3. **Communication**. Risks that result from poor communication are due to lack of knowledge of the system mission, requirements, and design goals and methods, or to lack of information about the importance of program goals to the company or the project.

2.5.4. **Morale**. Risks that result from low morale range across low levels of enthusiasm and thus low performance, productivity or creativity; anger that may result in intentional damage to the project or the product; mass exodus of staff from the project; and a reputation within the company that makes it difficult to recruit.

3. Program Constraints Class

The program constraints class consists of the "externals" of the project—the factors that are outside the direct control of the project but can still have major effects on its success. Program constraints include the following elements:

3.1. **Resources**: The external constraints imposed on schedule, staff, budget, or facilities.

3.1.1. **Schedule**. This attribute refers to the stability of the schedule with respect to internal and external events or dependencies and the viability of estimates and planning for all phases and aspects of the program.

3.1.2. **Staff.** This attribute refers to the stability and adequacy of the staff in terms of numbers and skill levels, their experience and skills in the required technical areas and application domain, and their availability when needed.

3.1.3. **Budget.** This attribute refers to the stability of the budget with respect to internal and external events or dependencies and the viability of estimates and planning for all phases and aspects of the program.

3.1.4. **Facilities**. This attribute refers to the adequacy of the program facilities for development, integration, and testing of the product.

3.2. **Contract**: The terms and conditions of the project contract.

3.2.1. **Type of Contract**. This attribute covers the payment terms (cost plus award fee, cost plus fixed fee, etc.) and the contractual requirements associated with such items as the Statement of Work, Contract Data Requirements List, and the amount and conditions of customer involvement.

3.2.2. **Restrictions.** Contract restrictions and restraints refer to contractual directives to, for example, use specific development methods or equipment and the resultant complications such as acquisition of data rights for use of non-developmental software.

3.2.3. **Dependencies**. This attribute refers to the possible contractual dependencies on outside contractors or vendors, customer-furnished equipment or software, or other outside products and services.

3.3. **Program Interfaces**: The external interfaces to customers, other contractors, corporate management, and vendors.

3.3.1. **Customer**. The customer attribute refers to the customer's level of skill and experience in the technical or application domain of the program as well as difficult working relationships or poor mechanisms for attaining customer agreement and approvals, not having access to certain customer factions, or not being able to communicate with the customer in a forthright manner.

3.3.2. **Associate Contractors.** The presence of associate contractors may introduce risks due to conflicting political agendas, problems of interfaces to systems being developed by outside organizations, or lack of cooperation in coordinating schedules and configuration changes.

3.3.3. **Subcontractors.** The presence of subcontractors may introduce risks due to inadequate task definitions and subcontractor management mechanisms, or to not transferring subcontractor technology and knowledge to the program or corporation.

3.3.4. **Prime Contractor**. When the program is a subcontract, risks may arise from poorly defined task definitions, complex reporting arrangements, or dependencies on technical or programmatic information.

3.3.5. **Corporate Management**. Risks in the corporate management area include poor communication and direction from senior management as well as non-optimum levels of support.

3.3.6. **Vendors**. Vendor risks may present themselves in the forms of dependencies on deliveries and support for critical system components.

3.3.7. **Politics**. Political risks may accrue from relationships with the company, customer, associate contractors or subcontractors, and may affect technical decisions.

APPENDIX B

TAXONOMY-BASED QUESTIONNAIRE [29]

A. Product Engineering

1. Requirements

a. Stability [Are requirements changing even as the product is being produced?]

[1] Are the requirements stable?

(No) (1.a) What is the effect on the system?

- Quality
- Functionality
- Schedule
- Integration
- Design
- Testing

[2] Are the external interfaces changing?

b. Completeness [Are requirements missing or incompletely specified?]

[3] Are there any TBDs in the specifications?

[4] Are there requirements you know should be in the specification but aren't?

(Yes) (4.a) Will you be able to get these requirements into the system?

[5] Does the customer have unwritten requirements/expectations?

(Yes) (5.a) Is there a way to capture these requirements?

[6] Are the external interfaces completely defined?

c. Clarity [Are requirements unclear or in need of interpretation?]

[7] Are you able to understand the requirements as written?

(No) (7.a) Are the ambiguities being resolved satisfactorily?

(Yes) (7.b) There are no ambiguities or problems of interpretation?

d. Validity [Will the requirements lead to the product the customer has in mind?]

[8] Are there any requirements that may not specify what the customer really wants?

(Yes) (8.a) How are you resolving this?

[9] Do you and the customer understand the same thing by the requirements?

(Yes) (9.a) Is there a process by which to determine this?

[10] How do you validate the requirements?

- Prototyping
- Analysis
- Simulations

e. Feasibility [Are requirements infeasible from an analytical point of view?]

[11] Are there any requirements that are technically difficult to implement?

(Yes) (11.a) What are they?

(Yes) (11.b) Why are they difficult to implement?

(No) (11.c) Were feasibility studies done for these requirements?

(Yes) (11.c.1) How confident are you of the assumptions made in the studies?

f. Precedent [Do requirements specify something never done before, or that your company has not done before?]

[12] Are there any state-of-the-art requirements?

- Technologies
- Methods
- Languages
- Hardware

(No) (12.a) Are any of these new to you?

(Yes) (12.b) Does the program have sufficient knowledge in these areas?

(No) (12.b.1) Is there a plan for acquiring knowledge in these areas?

g. Scale [Do requirements specify a product larger, more complex, or requiring a larger organization than in the experience of the company?]

[13] Is the system size and complexity a concern?

(No) (13.a) Have you done something of this size and complexity before?

[14] Does the size require a larger organization than usual for your company?

2. Design

a. Functionality [Are there any potential problems in meeting functionality requirements?]

[15] Are there any specified algorithms that may not satisfy the requirements?

(No) (15.a) Are any of the algorithms or designs marginal with respect to meeting requirements?

[16] How do you determine the feasibility of algorithms and designs?

- Prototyping
- Modeling
- Analysis
- Simulation

b. Difficulty [Will the design and/or implementation be difficult to achieve?]

[17] Does any of the design depend on unrealistic or optimistic assumptions?

[18] Are there any requirements or functions that are difficult to design?

(No) (18.a) Do you have solutions for all the requirements?

(Yes) (18.b) What are the requirements?

- Why are they difficult?

c. Interfaces [Are the internal interfaces (hardware and software) well defined and controlled?]

[19] Are the internal interfaces well defined?

- Software-to-software
- Software-to-hardware

[20] Is there a process for defining internal interfaces?

(Yes) (20.a) Is there a change control process for internal interfaces?

[21] Is hardware being developed in parallel with software?

(Yes) (21.a) Are the hardware specifications changing?

(Yes) (21.b) Have all the interfaces to software been defined?

(Yes) (21.c) Will there be engineering design models that can be used to test the software?

d. Performance [Are there stringent response time or throughput requirements?]

[22] Are there any problems with performance?

- Throughput
- Scheduling asynchronous real-time events
- Real-time response
- Recovery timelines
- Response time
- Database response, contention, or access

[23] Has a performance analysis been done?

(Yes) (23.a) What is your level of confidence in the performance analysis?

(Yes) (23.b) Do you have a model to track performance through design and implementation?

e. Testability [Is the product difficult or impossible to test?]

[24] Is the software going to be easy to test?

[25] Does the design include features to aid testing?

[26] Do the testers get involved in analyzing requirements?

f. Hardware Constraints [Are there tight constraints on the target hardware?]

[27] Does the hardware limit your ability to meet any requirements?

- Architecture
- Memory capacity
- Throughput
- Real-time response
- Response time
- Recovery timelines
- Database performance
- Functionality
- Reliability
- Availability

g. Non-Developmental Software [Are there problems with software used in the program but not developed by the program?]

If re-used or re-engineered software exists

[28] Are you reusing or re-engineering software not developed on the program?

(Yes) (28.a) Do you foresee any problems?

- Documentation
- Performance
- Functionality
- Timely delivery
- Customization

If COTS software is being used

[29] Are there any problems with using COTS (commercial off-the-shelf) software?

- Insufficient documentation to determine interfaces, size, or performance
- Poor performance
- Requires a large share of memory or database storage
- Difficult to interface with application software
- Not thoroughly tested

- Not bug free
- Not maintained adequately
- Slow vendor response

[30] Do you foresee any problem with integrating COTS software updates or revisions?

3. Code and Unit Test

a. Feasibility [Is the implementation of the design difficult or impossible?]

[31] Are any parts of the product implementation not completely defined by the design specification?

[32] Are the selected algorithms and designs easy to implement?

b. Testing [Are the specified level and time for unit testing adequate?]

[33] Do you begin unit testing before you verify code with respect to the design?

[34] Has sufficient unit testing been specified?

[35] Is there sufficient time to perform all the unit testing you think should be done?

[36] Will compromises be made regarding unit testing if there are schedule problems?

c. Coding/Implementation [Are there any problems with coding and implementation?]

[37] Are the design specifications in sufficient detail to write the code?

[38] Is the design changing while coding is being done?

[39] Are there system constraints that make the code difficult to write?

- Timing
- Memory
- External storage

[40] Is the language suitable for producing the software on this program?

[41] Are there multiple languages used on the program?

(Yes) (41.a) Is there interface compatibility between the code produced by the different compilers?

[42] Is the development computer the same as the target computer?

(No) (42.a) Are there compiler differences between the two?

If developmental hardware is being used

[43] Are the hardware specifications adequate to code the software?

[44] Are the hardware specifications changing while the code is being written?

4. Integration and Test

a. Environment [Is the integration and test environment adequate?]

[45] Will there be sufficient hardware to do adequate integration and testing?

[46] Is there any problem with developing realistic scenarios and test data to demonstrate any requirements?

- Specified data traffic
- Real-time response
- Asynchronous event handling
- Multi-user interaction

[47] Are you able to verify performance in your facility?

[48] Does hardware and software instrumentation facilitate testing?

(Yes) (48.a) Is it sufficient for all testing?

b. Product [Is the interface definition inadequate, facilities inadequate, time insufficient?]

[49] Will the target hardware be available when needed?

[50] Have acceptance criteria been agreed to for all requirements?

(Yes) (50.a) Is there a formal agreement?

[51] Are the external interfaces defined, documented, and baselined?

[52] Are there any requirements that will be difficult to test?

[53] Has sufficient product integration been specified?

[54] Has adequate time been allocated for product integration and test?

If COTS

[55] Will vendor data be accepted in verification of requirements allocated to COTS products?

(Yes) (55.a) Is the contract clear on that?

c. System [System integration uncoordinated, poor interface definition, or inadequate facilities?]

[56] Has sufficient system integration been specified?

[57] Has adequate time been allocated for system integration and test?

[58] Are all contractors part of the integration team?

[59] Will the product be integrated into an existing system?

(Yes) (59.a) Is there a parallel cutover period with the existing system?

(No) (59.a.1) How will you guarantee the product will work correctly when integrated?

[60] Will system integration occur on customer site?

5. Engineering Specialties

a. Maintainability [Will the implementation be difficult to understand or maintain?]

[61] Does the architecture, design, or code create any maintenance difficulties?

[62] Are the maintenance people involved early in the design?

[63] Is the product documentation adequate for maintenance by an outside organization?

b. Reliability [Are the reliability or availability requirements difficult to meet?]

[64] Are reliability requirements allocated to the software?

[65] Are availability requirements allocated to the software?

(Yes) (65.a) Are recovery timelines any problem?

c. Safety [Are the safety requirements infeasible and not demonstrable?]

[66] Are safety requirements allocated to the software?

(Yes) (66.a) Do you see any difficulty in meeting the safety requirements?

[67] Will it be difficult to verify satisfaction of safety requirements?

d. Security [Are the security requirements more stringent than the current state of the practice or program experience?]

[68] Are there unprecedented or state-of-the-art security requirements?

[69] Is it an Orange Book system?

[70] Have you implemented this level of security before?

e. Human Factors [Will the system will be difficult to use because of poor human interface definition?]

[71] Do you see any difficulty in meeting the Human Factors requirements?

(No) (71.a) How are you ensuring that you will meet the human interface requirements?

If prototyping

(Yes) (71.a.1) Is it a throw-away prototype?

(No) (71.a.1a) Are you doing evolutionary development?

(Yes) (71.a.1a.1) Are you experienced in this type of development?

(Yes) (71.a.1a.2) Are interim versions deliverable?

(Yes) (71.a.1a.3) Does this complicate change control?

f. Specifications [Is the documentation adequate to design, implement, and test the system?]

[72] Is the software requirements specification adequate to design the system?

[73] Are the hardware specifications adequate to design and implement the software?

[74] Are the external interface requirements well specified?

[75] Are the test specifications adequate to fully test the system?

If in or past implementation phase

[76] Are the design specifications adequate to implement the system?

- Internal interfaces

B. Development Environment

1. Development Process

a. Formality [Will the implementation be difficult to understand or maintain?]

[77] Is there more than one development model being used?

- Spiral
- Waterfall
- Incremental

(Yes) (77.a) Is coordination between them a problem?

[78] Are there formal, controlled plans for all development activities?

- Requirements analysis
- Design
- Code
- Integration and test
- Installation
- Quality assurance
- Configuration management

(Yes) (78.a) Do the plans specify the process well?

(Yes) (78.b) Are developers familiar with the plans?

b. Suitability [Is the process suited to the development model, e.g., spiral, prototyping?]

[79] Is the development process adequate for this product?

[80] Is the development process supported by a compatible set of procedures, methods, and tools?

c. Process Control [Is the software development process enforced, monitored, and controlled using metrics? Are distributed development sites coordinated?]

[81] Does everyone follow the development process?

(Yes) (81.a) How is this insured?

[82] Can you measure whether the development process is meeting your productivity and quality goals?

If there are distributed development sites

[83] Is there adequate coordination among distributed development sites?

d. Familiarity [Are the project members experienced in use of the process? Is the process understood by all staff members?]

[84] Are people comfortable with the development process?

e. Product Control [Are there mechanisms for controlling changes in the product?]

[85] Is there a requirements traceability mechanism that tracks requirements from the source specification through test cases?

[86] Is the traceability mechanism used in evaluating requirement change impact analyses?

[87] Is there a formal change control process?

(Yes) (87.a) Does it cover all changes to baselined requirements, design, code, and documentation?

[88] Are changes at any level mapped up to the system level and down through the test level?

[89] Is there adequate analysis when new requirements are added to the system?

[90] Do you have a way to track interfaces?

[91] Are the test plans and procedures updated as part of the change process?

2. Development System

a. Capacity [Is there sufficient work station processing power, memory, or storage capacity?]

[92] Are there enough workstations and processing capacity for all staff?

[93] Is there sufficient capacity for overlapping phases, such as coding, integration and test?

b. Suitability [Does the development system support all phases, activities, and functions?]

[94] Does the development system support all aspects of the program?

- Requirements analysis
- Performance analysis
- Design
- Coding
- Test

- Documentation
- Configuration management
- Management tracking
- Requirements traceability

c. Usability [How easy is the development system to use?]

[95] Do people find the development system easy to use?

[96] Is there good documentation of the development system?

d. Familiarity [Is there little prior company or project member experience with the development system?]

[97] Have people used these tools and methods before?

e. Reliability [Does the system suffer from software bugs, down-time, insufficient built-in back-up?]

[98] Is the system considered reliable?

- Compiler
- Development tools
- Hardware

f. System Support [Is there timely expert or vendor support for the system?]

[99] Are the people trained in use of the development tools?

[100] Do you have access to experts in use of the system?

[101] Do the vendors respond to problems rapidly?

g. Deliverability [Are the definition and acceptance requirements defined for delivering the development system to the customer not budgeted? HINT: If the participants are confused about this, it is probably not an issue from a risk perspective.]

[102] Are you delivering the development system to the customer?

(Yes) (102.a) Have adequate budget, schedule, and resources been allocated for this deliverable?

3. Management Process

a. Planning [Is the planning timely, technical leads included, contingency planning done?]

[103] Is the program managed according to the plan?

(Yes) (103.a) Do people routinely get pulled away to fight fires?

[104] Is re-planning done when disruptions occur?

[105] Are people at all levels included in planning their own work?

[106] Are there contingency plans for known risks?

(Yes) (106.a) How do you determine when to activate the contingencies?

[107] Are long-term issues being adequately addressed?

b. Project Organization [Are the roles and reporting relationships clear?]

[108] Is the program organization effective?

[109] Do people understand their own and others' roles in the program?

[110] Do people know who has authority for what?

c. Management Experience [Are the managers experienced in software development, software management, the application domain, the development process, or on large programs?]

[111] Does the program have experienced managers?

- Software management
- Hands-on software development
- With this development process
- In the application domain
- Program size or complexity

d. Program Interfaces [Is there poor interface with customer, other contractors, senior and/or peer managers?]

[112] Does management communicate problems up and down the line?

[113] Are conflicts with the customer documented and resolved in a timely manner?

[114] Does management involve appropriate program members in meetings with the customer?

- Technical leaders
- Developers
- Analysts

[115] Does management work to ensure that all customer factions are represented in decisions regarding functionality and operation?

[116] Is it good politics to present an optimistic picture to the customer or senior management?

4. Management Methods

a. Monitoring [Are management metrics defined and development progress tracked?]

[117] Are there periodic structured status reports?

(Yes) (117.a) Do people get a response to their status reports?

[118] Does appropriate information get reported to the right organizational levels?

[119] Do you track progress versus plan?

(Yes) (119.a) Does management have a clear picture of what is going on?

b. Personnel Management [Are project personnel trained and used appropriately?]

[120] Do people get trained in skills required for this program?

(Yes) (120.a) Is this part of the program plan?

[121] Do people get assigned to the program, who do not match the experience profile for your work area?

[122] Is it easy for program members to get management action?

[123] Are program members at all levels aware of their status versus plan?

[124] Do people feel it's important to keep to the plan?

[125] Does management consult with people before making decisions that affect their work?

[126] Does program management involve appropriate program members in meetings with the customer?

- Technical leaders
- Developers
- Analysts

c. Quality Assurance [Are there adequate procedures and resources to assure product quality?]

[127] Is the software quality assurance function adequately staffed on this program?

[128] Do you have defined mechanisms for assuring quality?

(Yes) (128.a) Do all areas and phases have quality procedures?

(Yes) (128.b) Are people used to working with these procedures?

d. Configuration Management [Are the change procedures or version control, including installation site(s), adequate?]

[129] Do you have an adequate configuration management system?

[130] Is the configuration management function adequately staffed?

[131] Is coordination required with an installed system?

(Yes) (131.a) Is there adequate configuration management of the installed system?

(Yes) (131.b) Does the configuration management system synchronize your work with site changes?

[132] Are you installing in multiple sites?

(Yes) (132.a) Does the configuration management system provide for multiple sites?

5. Work Environment

a. Quality Attitude [Is there a lack of orientation toward quality work?]

[133] Are all staff levels oriented toward quality procedures?

[134] Does schedule get in the way of quality?

b. Cooperation [Is there a lack of team spirit? Does conflict resolution require management intervention?]

[135] Do people work cooperatively across functional boundaries?

[136] Do people work effectively toward common goals?

[137] Is management intervention sometimes required to get people working together?

c. Communication [Is there poor awareness of mission or goals, poor communication of technical information among peers and managers?]

[138] Is there good communication among the members of the program?

- Managers
- Technical leaders
- Developers
- Testers
- Configuration management
- Quality assurance

[139] Are the managers receptive to communication from program staff?

(Yes) (139.a) Do you feel free to ask your managers for help?

(Yes) (139.b) Are members of the program able to raise risks without having a solution in hand?

[140] Do the program members get timely notification of events that may affect their work?

(Yes) (140.a) Is this formal or informal?

d. Morale [Is there a non-productive, non-creative atmosphere? Do people feel that there is no recognition or reward for superior work?]

[141] How is morale on the program?

(No) (141.a) What is the main contributing factor to low morale?

[142] Is there any problem keeping the people you need?

C. Program Constraints

1. Resources

a. Schedule [Is the schedule inadequate or unstable?]

[143] Has the schedule been stable?

[144] Is the schedule realistic?

(Yes) (144.a) Is the estimation method based on historical data?

(Yes) (144.b) Has the method worked well in the past?

[145] Is there anything for which adequate schedule was not planned?

- Analysis and studies
- QA
- Training
- Maintenance courses and training
- Capital equipment
- Deliverable development system

[146] Are there external dependencies which are likely to impact the schedule?

b. Staff [Is the staff inexperienced, lacking domain knowledge, lacking skills, or understaffed?]

[147] Are there any areas in which the required technical skills are lacking?

- Software engineering and requirements analysis method
- Algorithm expertise
- Design and design methods
- Programming languages
- Integration and test methods
- Reliability
- Maintainability
- Availability
- Human factors
- Configuration management
- Quality assurance
- Target environment
- Level of security
- COTS
- Reuse software
- Operating system
- Database
- Application domain
- Performance analysis

- Time-critical applications

[148] Do you have adequate personnel to staff the program?

[149] Is the staffing stable?

[150] Do you have access to the right people when you need them?

[151] Have the program members implemented systems of this type?

[152] Is the program reliant on a few key people?

[153] Is there any problem with getting cleared people?

c. Budget [Is the funding insufficient or unstable?]

[154] Is the budget stable?

[155] Is the budget based on a realistic estimate?

(Yes) (155.a) Is the estimation method based on historical data?

(Yes) (155.b) Has the method worked well in the past?

[156] Have features or functions been deleted as part of a design-to-cost effort?

[157] Is there anything for which adequate budget was not allocated?

- Analysis and studies
- QA
- Training
- Maintenance courses
- Capital equipment
- Deliverable development system

[158] Do budget changes accompany requirement changes?

(Yes) (158.a) Is this a standard part of the change control process?

d. Facilities [Are the facilities adequate for building and delivering the product?]

[159] Are the development facilities adequate?

[160] Is the integration environment adequate?

2. Contract

a. Type of Contract [Is the contract type a source of risk to the program?]

[161] What type of contract do you have? (Cost plus award fee, fixed price,....)

(161a) Does this present any problems?

[162] Is the contract burdensome in any aspect of the program?

- SOW (Statement of Work)
- Specifications
- DIDs (Data Item Descriptions)
- Contract parts
- Excessive customer involvement

[163] Is the required documentation burdensome?

- Excessive amount
- Picky customer
- Long approval cycle

b. Restrictions [Does the contract cause any restrictions?]

[164] Are there problems with data rights?

- COTS software
- Developmental software
- Non-developmental items

c. Dependencies [Does the program have any dependencies on outside products or services?]

[165] Are there dependencies on external products or services that may affect the product, budget, or schedule?

- Associate contractors
- Prime contractor
- Subcontractors
- Vendors or suppliers
- Customer furnished equipment or software

3. Program Interfaces

a. Customer [Are there any customer problems such as: lengthy document-approval cycle, poor communication, and inadequate domain expertise?]

[166] Is the customer approval cycle timely?

- Documentation
- Program reviews
- Formal reviews

[167] Do you ever proceed before receiving customer approval?

[168] Does the customer understand the technical aspects of the system?

[169] Does the customer understand software?

[170] Does the customer interfere with process or people?

[171] Does management work with the customer to reach mutually agreeable decisions in a timely manner?

- Requirements understanding
- Test criteria
- Schedule adjustments
- Interfaces

[172] How effective are your mechanisms for reaching agreements with the customer?

- Working groups (contractual?)
- Technical interchange meetings (contractual?)

[173] Are all customer factions involved in reaching agreements?

(Yes) (173.a) Is it a formally defined process?

[174] Does management present a realistic or optimistic picture to the customer?

If there are associate contractors

b. Associate Contractors [Are there any problems with associate contractors such as inadequately defined or unstable interfaces, poor communication, or lack of cooperation?]

[175] Are the external interfaces changing without adequate notification, coordination, or

formal change procedures?

[176] Is there an adequate transition plan?

(Yes) (176.a) Is it supported by all contractors and site personnel?

[177] Is there any problem with getting schedules or interface data from associate contractors?

(No) (177.a) Are they accurate?

If there are subcontractors

c. Subcontractors [Is the program dependent on subcontractors for any critical areas?]

[178] Are there any ambiguities in subcontractor task definitions?

[179] Is the subcontractor reporting and monitoring procedure different from the program's reporting requirements?

[180] Is subcontractor administration and technical management done by a separate organization?

[181] Are you highly dependent on subcontractor expertise in any areas?

[182] Is subcontractor knowledge being transferred to the company?

[183] Is there any problem with getting schedules or interface data from subcontractors?

If program is a subcontract

d. Prime Contractor [Is the program facing difficulties with its Prime contractor?]

[184] Are your task definitions from the Prime ambiguous?

[185] Do you interface with two separate prime organizations for administration and technical management?

[186] Are you highly dependent on the Prime for expertise in any areas?

[187] Is there any problem with getting schedules or interface data from the Prime?

e. Corporate Management [Is there a lack of support or micro management from upper management?]

[188] Does program management communicate problems to senior management?

(Yes) (188.a) Does this seem to be effective?

[189] Does corporate management give you timely support in solving your problems?

[190] Does corporate management tend to micro-manage?

[191] Does management present a realistic or optimistic picture to senior management?

f. Vendors [Are vendors responsive to programs needs?]

[192] Are you relying on vendors for deliveries of critical components?

- Compilers
- Hardware
- COTS

g. Politics [Are politics causing a problem for the program?]

[193] Are politics affecting the program?

- Company
- Customer
- Associate contractors
- Subcontractors

[194] Are politics affecting technical decisions?

APPENDIX C

PRIORITIZATION OF THE RISK ITEMS FOR EACH CLASS AND WHOLE SET IN ACCORDANCE WITH RISK PRIORITIZATION METHODS

Table 22 'Product Engineering' Risks Sorted iaw Risk Prioritization Method 1

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. For Mitigation	Exposure /Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
1	5.6	16	0.5	0.350	0.175
5	5.6	144	0.7	0.039	0.027
25	5.4	64	0.7	0.084	0.059
6	4.9	160	0.8	0.031	0.025
36	4.5	120	0.8	0.038	0.030
10	4.2	40	0.9	0.105	0.095
15	4.2	40	0.7	0.105	0.074
33	4.2	80	0.8	0.053	0.042
2	3.5	48	0.7	0.073	0.051
9	3.5	120	0.6	0.029	0.018
21	3.5	48	0.6	0.073	0.044
32	3.5	96	0.8	0.036	0.029
4	3.0	16	0.5	0.188	0.094
19	3.0	120	0.8	0.025	0.020
31	3.0	160	0.8	0.019	0.015
23	2.8	16	0.5	0.175	0.088
37	2.8	80	0.7	0.035	0.025
39	2.8	80	0.7	0.035	0.025
24	2.5	64	0.6	0.039	0.023
3	2.4	32	0.7	0.075	0.053
11	2.4	200	0.8	0.012	0.010
29	2.1	8	0.3	0.263	0.079
38	2.1	80	0.7	0.026	0.018
13	2.0	24	0.6	0.083	0.050
14	2.0	40	0.9	0.050	0.045

Table 22 ‘Product Engineering’ Risks Sorted iaw Risk Prioritization Method 1 (cont’d)

26	2.0	48	0.6	0.042	0.025
34	2.0	64	0.7	0.031	0.022
7	1.8	80	0.8	0.023	0.018
12	1.5	32	0.9	0.047	0.042
30	1.5	64	0.6	0.023	0.016
41	1.5	64	0.7	0.023	0.014
20	1.5	16	0.5	0.094	0.047
35	1.5	72	0.9	0.021	0.019
16	1.2	32	0.7	0.038	0.026
18	1.2	72	0.8	0.017	0.013
42	1.2	96	0.8	0.013	0.010
28	0.9	16	0.9	0.056	0.051
22	0.6	16	0.8	0.038	0.030
27	0.6	32	0.8	0.019	0.015
40	0.6	72	0.6	0.008	0.005
8	0.5	12	0.9	0.042	0.038
17	0.5	20	0.9	0.025	0.023

Table 23 ‘Development Environment’ Risks Sorted iaw Risk Prioritization Method 1

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. for Mitigation	Exposure /Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
59	7.2	136	0.9	0.053	0.048
69	5.4	20	0.8	0.270	0.216
70	5.4	27	0.8	0.200	0.160
58	4.9	40	0.8	0.123	0.098
60	4.9	40	0.8	0.123	0.098
67	4.2	112	0.9	0.038	0.034
43	3.5	112	0.9	0.031	0.028
54	3.5	48	0.7	0.073	0.051
57	3.5	16	0.6	0.219	0.131
49	3.5	16	0.6	0.219	0.131
53	3.5	64	0.6	0.055	0.033
62	3.5	16	0.5	0.219	0.109
48	3.0	96	0.8	0.031	0.025
56	3.0	16	0.5	0.188	0.094
63	2.8	40	0.7	0.070	0.049
61	2.5	32	0.6	0.078	0.047
64	2.5	16	0.5	0.156	0.078
45	2.4	40	0.9	0.060	0.054
55	2.4	8	0.8	0.300	0.240
46	2.0	32	0.8	0.063	0.050
65	2.0	40	0.7	0.050	0.035
50	1.8	16	0.5	0.113	0.056
52	1.5	64	0.6	0.023	0.014
44	1.5	32	0.8	0.047	0.038
47	1.4	40	0.9	0.035	0.032
51	1.2	28	0.9	0.043	0.039
66	0.9	32	0.8	0.028	0.023
71	0.9	40	0.9	0.023	0.020
68	0.6	8	0.8	0.075	0.060

Table 24 'Program Constraints' Risks Sorted iaw Risk Prioritization Method 1

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. for Mitigation	Exposure/Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
85	7.2	160	0.8	0.045	0.036
101	5.6	32	0.6	0.175	0.105
73	5.4	12	0.7	0.450	0.315
94	5.4	16	0.5	0.338	0.169
87	4.9	48	0.7	0.102	0.071
77	4.2	20	0.8	0.105	0.168
88	4.2	72	0.6	0.058	0.035
79	4.0	205	0.9	0.020	0.018
92	4.0	24	0.6	0.167	0.100
74	3.5	24	0.4	0.146	0.058
78	3.5	205	0.9	0.017	0.015
86	3.5	32	0.6	0.109	0.066
95	3.5	16	0.5	0.219	0.109
97	3.5	16	0.5	0.219	0.109
93	3.5	16	0.5	0.219	0.109
75	3.0	24	0.4	0.125	0.050
100	3.0	16	0.5	0.188	0.094
76	2.5	40	0.6	0.063	0.038
96	2.4	16	0.5	0.150	0.075
81	2.1	205	0.9	0.010	0.009
91	2.1	16	0.5	0.131	0.066
72	2.0	16	0.9	0.125	0.113
82	2.0	8	0.8	0.250	0.200
84	2.0	16	0.5	0.125	0.063
90	2.0	40	0.8	0.050	0.040
99	1.8	24	0.6	0.075	0.045
83	1.5	72	0.7	0.021	0.015
89	1.5	12	0.5	0.125	0.063
98	1.5	16	0.5	0.094	0.047
80	1.2	24	0.9	0.050	0.045
102	1.0	20	0.7	0.050	0.035

Table 25 Whole Set of Risks Sorted iaw Risk Prioritization Method 1

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. for Mitigation	Exposure/ Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
59	7.2	136	0.9	0.053	0.048
85	7.2	160	0.8	0.045	0.036
1	5.6	16	0.5	0.350	0.175
5	5.6	144	0.7	0.039	0.027
101	5.6	32	0.6	0.175	0.105
25	5.4	64	0.7	0.084	0.059
69	5.4	20	0.8	0.270	0.216
70	5.4	27	0.8	0.200	0.160
73	5.4	12	0.7	0.450	0.315
94	5.4	16	0.5	0.338	0.169
6	4.9	160	0.8	0.031	0.025
58	4.9	40	0.8	0.123	0.098
60	4.9	40	0.8	0.123	0.098
87	4.9	48	0.7	0.102	0.071
36	4.5	120	0.8	0.038	0.030
10	4.2	40	0.9	0.105	0.095
15	4.2	40	0.7	0.105	0.074
33	4.2	80	0.8	0.053	0.042
67	4.2	112	0.9	0.038	0.034
77	4.2	20	0.8	0.105	0.084
88	4.2	72	0.6	0.058	0.035
79	4.0	205	0.9	0.020	0.018
92	4.0	24	0.6	0.167	0.100
2	3.5	48	0.7	0.073	0.051
9	3.5	120	0.6	0.029	0.018
43	3.5	112	0.9	0.031	0.028
54	3.5	48	0.7	0.073	0.051
57	3.5	16	0.6	0.219	0.131
74	3.5	24	0.4	0.146	0.058
78	3.5	205	0.9	0.017	0.015
86	3.5	32	0.6	0.109	0.066
95	3.5	16	0.5	0.219	0.109
97	3.5	16	0.5	0.219	0.109
21	3.5	48	0.6	0.073	0.044
32	3.5	96	0.8	0.036	0.029
49	3.5	16	0.6	0.219	0.131

Table 25 Whole Set of Risks Sorted iaw Risk Prioritization Method 1 (cont'd)

53	3.5	64	0.6	0.055	0.033
62	3.5	16	0.5	0.219	0.109
93	3.5	16	0.5	0.219	0.109
4	3.0	16	0.5	0.188	0.094
19	3.0	120	0.8	0.025	0.020
31	3.0	160	0.8	0.019	0.015
48	3.0	96	0.8	0.031	0.025
56	3.0	16	0.5	0.188	0.094
75	3.0	24	0.4	0.125	0.050
100	3.0	16	0.5	0.188	0.094
23	2.8	16	0.5	0.175	0.088
37	2.8	80	0.7	0.035	0.025
39	2.8	80	0.7	0.035	0.025
63	2.8	40	0.7	0.070	0.049
24	2.5	64	0.6	0.039	0.023
61	2.5	32	0.6	0.078	0.047
64	2.5	16	0.5	0.156	0.078
76	2.5	40	0.6	0.063	0.038
3	2.4	32	0.7	0.075	0.053
11	2.4	200	0.8	0.012	0.010
45	2.4	40	0.9	0.060	0.054
55	2.4	8	0.8	0.300	0.240
96	2.4	16	0.5	0.150	0.075
29	2.1	8	0.3	0.263	0.079
81	2.1	205	0.9	0.010	0.009
38	2.1	80	0.7	0.026	0.018
91	2.1	16	0.5	0.131	0.066
13	2.0	24	0.6	0.083	0.050
14	2.0	40	0.9	0.050	0.045
26	2.0	48	0.6	0.042	0.025
34	2.0	64	0.7	0.031	0.022
46	2.0	32	0.8	0.063	0.050
65	2.0	40	0.7	0.050	0.035
72	2.0	16	0.9	0.125	0.113
82	2.0	8	0.8	0.250	0.200
84	2.0	16	0.5	0.125	0.063
90	2.0	40	0.8	0.050	0.040
7	1.8	80	0.8	0.023	0.018
50	1.8	16	0.5	0.113	0.056
99	1.8	24	0.6	0.075	0.045
12	1.5	32	0.9	0.047	0.042
30	1.5	64	0.6	0.023	0.016
41	1.5	64	0.7	0.023	0.014
52	1.5	64	0.6	0.023	0.014

Table 25 Whole Set of Risks Sorted iaw Risk Prioritization Method 1 (cont'd)

83	1.5	72	0.7	0.021	0.015
89	1.5	12	0.5	0.125	0.063
98	1.5	16	0.5	0.094	0.047
20	1.5	16	0.5	0.094	0.047
35	1.5	72	0.9	0.021	0.019
44	1.5	32	0.8	0.047	0.038
47	1.4	40	0.9	0.035	0.032
16	1.2	32	0.7	0.038	0.026
18	1.2	72	0.8	0.017	0.013
42	1.2	96	0.8	0.013	0.010
51	1.2	28	0.9	0.043	0.039
80	1.2	24	0.9	0.050	0.045
102	1.0	20	0.7	0.050	0.035
28	0.9	16	0.9	0.056	0.051
66	0.9	32	0.8	0.028	0.023
71	0.9	40	0.9	0.023	0.020
22	0.6	16	0.8	0.038	0.030
27	0.6	32	0.8	0.019	0.015
40	0.6	72	0.6	0.008	0.005
68	0.6	8	0.8	0.075	0.060
8	0.5	12	0.9	0.042	0.038
17	0.5	20	0.9	0.025	0.023

Table 26 ‘Product Engineering’ Risks Sorted iaw Risk Prioritization Method 2

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. for Mitigation	Exposure/ Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
1	5.6	16	0.5	0.350	0.175
29	2.1	8	0.3	0.263	0.079
4	3.0	16	0.5	0.188	0.094
23	2.8	16	0.5	0.175	0.088
10	4.2	40	0.9	0.105	0.095
15	4.2	40	0.7	0.105	0.074
20	1.5	16	0.5	0.094	0.047
25	5.4	64	0.7	0.084	0.059
13	2.0	24	0.6	0.083	0.050
3	2.4	32	0.7	0.075	0.053
2	3.5	48	0.7	0.073	0.051
21	3.5	48	0.6	0.073	0.044
28	0.9	16	0.9	0.056	0.051
33	4.2	80	0.8	0.053	0.042
14	2.0	40	0.9	0.050	0.045
12	1.5	32	0.9	0.047	0.042
26	2.0	48	0.6	0.042	0.025
8	0.5	12	0.9	0.042	0.038
24	2.5	64	0.6	0.039	0.023
5	5.6	144	0.7	0.039	0.027
36	4.5	120	0.8	0.038	0.030
16	1.2	32	0.7	0.038	0.026
22	0.6	16	0.8	0.038	0.030
32	3.5	96	0.8	0.036	0.029
37	2.8	80	0.7	0.035	0.025
39	2.8	80	0.7	0.035	0.025
34	2.0	64	0.7	0.031	0.022
6	4.9	160	0.8	0.031	0.025
9	3.5	120	0.6	0.029	0.018
38	2.1	80	0.7	0.026	0.018
19	3.0	120	0.8	0.025	0.020
17	0.5	20	0.9	0.025	0.023
30	1.5	64	0.6	0.023	0.016
41	1.5	64	0.7	0.023	0.014
7	1.8	80	0.8	0.023	0.018
35	1.5	72	0.9	0.021	0.019
31	3.0	160	0.8	0.019	0.015
27	0.6	32	0.8	0.019	0.015

Table 26 ‘Product Engineering’ Risks Sorted iaw Risk Prioritization Method 2 (cont’d)

18	1.2	72	0.8	0.017	0.013
42	1.2	96	0.8	0.013	0.010
11	2.4	200	0.8	0.012	0.010
40	0.6	72	0.6	0.008	0.005

Table 27 ‘Development Environment’ Risks Sorted iaw Risk Prioritization Method 2

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. for Mitigation	Exposure/ Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
55	2.4	8	0.8	0.300	0.240
69	5.4	20	0.8	0.270	0.216
57	3.5	16	0.6	0.219	0.131
49	3.5	16	0.6	0.219	0.131
62	3.5	16	0.5	0.219	0.109
70	5.4	27	0.8	0.200	0.160
56	3.0	16	0.5	0.188	0.094
64	2.5	16	0.5	0.156	0.078
58	4.9	40	0.8	0.123	0.098
60	4.9	40	0.8	0.123	0.098
50	1.8	16	0.5	0.113	0.056
61	2.5	32	0.6	0.078	0.047
68	0.6	8	0.8	0.075	0.060
54	3.5	48	0.7	0.073	0.051
63	2.8	40	0.7	0.070	0.049
46	2.0	32	0.8	0.063	0.050
45	2.4	40	0.9	0.060	0.054
53	3.5	64	0.6	0.055	0.033
59	7.2	136	0.9	0.053	0.048
65	2.0	40	0.7	0.050	0.035
44	1.5	32	0.8	0.047	0.038
51	1.2	28	0.9	0.043	0.039
67	4.2	112	0.9	0.038	0.034
47	1.4	40	0.9	0.035	0.032
43	3.5	112	0.9	0.031	0.028
48	3.0	96	0.8	0.031	0.025
66	0.9	32	0.8	0.028	0.023
52	1.5	64	0.6	0.023	0.014
71	0.9	40	0.9	0.023	0.020

Table 28 'Program Constraints' Risks Sorted iaw Risk Prioritization Method 2

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. for Mitigation	Exposure/ Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
73	5.4	12	0.7	0.450	0.315
94	5.4	16	0.5	0.338	0.169
82	2.0	8	0.8	0.250	0.200
95	3.5	16	0.5	0.219	0.109
97	3.5	16	0.5	0.219	0.109
93	3.5	16	0.5	0.219	0.109
100	3.0	16	0.5	0.188	0.094
101	5.6	32	0.6	0.175	0.105
92	4.0	24	0.6	0.167	0.100
96	2.4	16	0.5	0.150	0.075
74	3.5	24	0.4	0.146	0.058
91	2.1	16	0.5	0.131	0.066
75	3.0	24	0.4	0.125	0.050
72	2.0	16	0.9	0.125	0.113
84	2.0	16	0.5	0.125	0.063
89	1.5	12	0.5	0.125	0.063
86	3.5	32	0.6	0.109	0.066
77	4.2	20	0.8	0.105	0.168
87	4.9	48	0.7	0.102	0.071
98	1.5	16	0.5	0.094	0.047
99	1.8	24	0.6	0.075	0.045
76	2.5	40	0.6	0.063	0.038
88	4.2	72	0.6	0.058	0.035
90	2.0	40	0.8	0.050	0.040
80	1.2	24	0.9	0.050	0.045
102	1.0	20	0.7	0.050	0.035
85	7.2	160	0.8	0.045	0.036
83	1.5	72	0.7	0.021	0.015
79	4.0	205	0.9	0.020	0.018
78	3.5	205	0.9	0.017	0.015
81	2.1	205	0.9	0.010	0.009

Table 29 Whole Set of Risks Sorted iaw Risk Prioritization Method 2

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. for Mitigation	Exposure/ Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
73	5.4	12	0.7	0.450	0.315
1	5.6	16	0.5	0.350	0.175
94	5.4	16	0.5	0.338	0.169
55	2.4	8	0.8	0.300	0.240
69	5.4	20	0.8	0.270	0.216
29	2.1	8	0.3	0.263	0.079
82	2.0	8	0.8	0.250	0.200
57	3.5	16	0.6	0.219	0.131
95	3.5	16	0.5	0.219	0.109
97	3.5	16	0.5	0.219	0.109
49	3.5	16	0.6	0.219	0.131
62	3.5	16	0.5	0.219	0.109
93	3.5	16	0.5	0.219	0.109
70	5.4	27	0.8	0.200	0.160
4	3.0	16	0.5	0.188	0.094
56	3.0	16	0.5	0.188	0.094
100	3.0	16	0.5	0.188	0.094
101	5.6	32	0.6	0.175	0.105
23	2.8	16	0.5	0.175	0.088
92	4.0	24	0.6	0.167	0.100
64	2.5	16	0.5	0.156	0.078
96	2.4	16	0.5	0.150	0.075
74	3.5	24	0.4	0.146	0.058
91	2.1	16	0.5	0.131	0.066
75	3.0	24	0.4	0.125	0.050
72	2.0	16	0.9	0.125	0.113
84	2.0	16	0.5	0.125	0.063
89	1.5	12	0.5	0.125	0.063
58	4.9	40	0.8	0.123	0.098
60	4.9	40	0.8	0.123	0.098
50	1.8	16	0.5	0.113	0.056
86	3.5	32	0.6	0.109	0.066
10	4.2	40	0.9	0.105	0.095
15	4.2	40	0.7	0.105	0.074
77	4.2	20	0.8	0.105	0.084
87	4.9	48	0.7	0.102	0.071
98	1.5	16	0.5	0.094	0.047

Table 29 Whole Set of Risks Sorted iaw Risk Prioritization Method 2 (cont'd)

20	1.5	16	0.5	0.094	0.047
25	5.4	64	0.7	0.084	0.059
13	2.0	24	0.6	0.083	0.050
61	2.5	32	0.6	0.078	0.047
3	2.4	32	0.7	0.075	0.053
99	1.8	24	0.6	0.075	0.045
68	0.6	8	0.8	0.075	0.060
2	3.5	48	0.7	0.073	0.051
54	3.5	48	0.7	0.073	0.051
21	3.5	48	0.6	0.073	0.044
63	2.8	40	0.7	0.070	0.049
76	2.5	40	0.6	0.063	0.038
46	2.0	32	0.8	0.063	0.050
45	2.4	40	0.9	0.060	0.054
88	4.2	72	0.6	0.058	0.035
28	0.9	16	0.9	0.056	0.051
53	3.5	64	0.6	0.055	0.033
59	7.2	136	0.9	0.053	0.048
33	4.2	80	0.8	0.053	0.042
14	2.0	40	0.9	0.050	0.045
65	2.0	40	0.7	0.050	0.035
90	2.0	40	0.8	0.050	0.040
80	1.2	24	0.9	0.050	0.045
102	1.0	20	0.7	0.050	0.035
12	1.5	32	0.9	0.047	0.042
44	1.5	32	0.8	0.047	0.038
85	7.2	160	0.8	0.045	0.036
51	1.2	28	0.9	0.043	0.039
26	2.0	48	0.6	0.042	0.025
8	0.5	12	0.9	0.042	0.038
24	2.5	64	0.6	0.039	0.023
5	5.6	144	0.7	0.039	0.027
36	4.5	120	0.8	0.038	0.030
67	4.2	112	0.9	0.038	0.034
16	1.2	32	0.7	0.038	0.026
22	0.6	16	0.8	0.038	0.030
32	3.5	96	0.8	0.036	0.029
37	2.8	80	0.7	0.035	0.025
39	2.8	80	0.7	0.035	0.025
47	1.4	40	0.9	0.035	0.032
43	3.5	112	0.9	0.031	0.028
48	3.0	96	0.8	0.031	0.025
34	2.0	64	0.7	0.031	0.022
6	4.9	160	0.8	0.031	0.025

Table 29 Whole Set of Risks Sorted iaw Risk Prioritization Method 2 (cont'd)

9	3.5	120	0.6	0.029	0.018
66	0.9	32	0.8	0.028	0.023
38	2.1	80	0.7	0.026	0.018
19	3.0	120	0.8	0.025	0.020
17	0.5	20	0.9	0.025	0.023
30	1.5	64	0.6	0.023	0.016
41	1.5	64	0.7	0.023	0.014
52	1.5	64	0.6	0.023	0.014
7	1.8	80	0.8	0.023	0.018
71	0.9	40	0.9	0.023	0.020
83	1.5	72	0.7	0.021	0.015
35	1.5	72	0.9	0.021	0.019
79	4.0	205	0.9	0.020	0.018
31	3.0	160	0.8	0.019	0.015
27	0.6	32	0.8	0.019	0.015
78	3.5	205	0.9	0.017	0.015
18	1.2	72	0.8	0.017	0.013
42	1.2	96	0.8	0.013	0.010
11	2.4	200	0.8	0.012	0.010
81	2.1	205	0.9	0.010	0.009
40	0.6	72	0.6	0.008	0.005

Table 30 ‘Product Engineering’ Risks Sorted iaw Risk Prioritization Method 3

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. for Mitigation	Exposure/Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
1	5.6	16	0.5	0.350	0.175
10	4.2	40	0.9	0.105	0.095
4	3.0	16	0.5	0.188	0.094
23	2.8	16	0.5	0.175	0.088
29	2.1	8	0.3	0.263	0.079
15	4.2	40	0.7	0.105	0.074
25	5.4	64	0.7	0.084	0.059
3	2.4	32	0.7	0.075	0.053
2	3.5	48	0.7	0.073	0.051
28	0.9	16	0.9	0.056	0.051
13	2.0	24	0.6	0.083	0.050
20	1.5	16	0.5	0.094	0.047
14	2.0	40	0.9	0.050	0.045
21	3.5	48	0.6	0.073	0.044
12	1.5	32	0.9	0.047	0.042
33	4.2	80	0.8	0.053	0.042
8	0.5	12	0.9	0.042	0.038
36	4.5	120	0.8	0.038	0.030
22	0.6	16	0.8	0.038	0.030
32	3.5	96	0.8	0.036	0.029
5	5.6	144	0.7	0.039	0.027
16	1.2	32	0.7	0.038	0.026
26	2.0	48	0.6	0.042	0.025
6	4.9	160	0.8	0.031	0.025
37	2.8	80	0.7	0.035	0.025
39	2.8	80	0.7	0.035	0.025
24	2.5	64	0.6	0.039	0.023
17	0.5	20	0.9	0.025	0.023
34	2.0	64	0.7	0.031	0.022
19	3.0	120	0.8	0.025	0.020
35	1.5	72	0.9	0.021	0.019
38	2.1	80	0.7	0.026	0.018
7	1.8	80	0.8	0.023	0.018
9	3.5	120	0.6	0.029	0.018
30	1.5	64	0.6	0.023	0.016
31	3.0	160	0.8	0.019	0.015
27	0.6	32	0.8	0.019	0.015

Table 30 ‘Product Engineering’ Risks Sorted iaw Risk Prioritization Method 3 (cont’d)

41	1.5	64	0.7	0.023	0.014
18	1.2	72	0.8	0.017	0.013
42	1.2	96	0.8	0.013	0.010
11	2.4	200	0.8	0.012	0.010
40	0.6	72	0.6	0.008	0.005

Table 31 ‘Development Environment’ Risks Sorted iaw Risk Prioritization Method 3

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. for Mitigation	Exposure/Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
55	2.4	8	0.8	0.300	0.240
69	5.4	20	0.8	0.270	0.216
70	5.4	27	0.8	0.200	0.160
57	3.5	16	0.6	0.219	0.131
49	3.5	16	0.6	0.219	0.131
62	3.5	16	0.5	0.219	0.109
58	4.9	40	0.8	0.123	0.098
60	4.9	40	0.8	0.123	0.098
56	3.0	16	0.5	0.188	0.094
64	2.5	16	0.5	0.156	0.078
68	0.6	8	0.8	0.075	0.060
50	1.8	16	0.5	0.113	0.056
45	2.4	40	0.9	0.060	0.054
54	3.5	48	0.7	0.073	0.051
46	2.0	32	0.8	0.063	0.050
63	2.8	40	0.7	0.070	0.049
59	7.2	136	0.9	0.053	0.048
61	2.5	32	0.6	0.078	0.047
51	1.2	28	0.9	0.043	0.039
44	1.5	32	0.8	0.047	0.038
65	2.0	40	0.7	0.050	0.035
67	4.2	112	0.9	0.038	0.034
53	3.5	64	0.6	0.055	0.033
47	1.4	40	0.9	0.035	0.032
43	3.5	112	0.9	0.031	0.028
48	3.0	96	0.8	0.031	0.025
66	0.9	32	0.8	0.028	0.023
71	0.9	40	0.9	0.023	0.020
52	1.5	64	0.6	0.023	0.014

Table 32 ‘Program Constraints’ Risks Sorted iaw Risk Prioritization Method 3

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. for Mitigation	Exposure/ Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
73	5.4	12	0.7	0.450	0.315
82	2.0	8	0.8	0.250	0.200
94	5.4	16	0.5	0.338	0.169
77	4.2	20	0.8	0.105	0.168
72	2.0	16	0.9	0.125	0.113
95	3.5	16	0.5	0.219	0.109
97	3.5	16	0.5	0.219	0.109
93	3.5	16	0.5	0.219	0.109
101	5.6	32	0.6	0.175	0.105
92	4.0	24	0.6	0.167	0.100
100	3.0	16	0.5	0.188	0.094
96	2.4	16	0.5	0.150	0.075
87	4.9	48	0.7	0.102	0.071
86	3.5	32	0.6	0.109	0.066
91	2.1	16	0.5	0.131	0.066
84	2.0	16	0.5	0.125	0.063
89	1.5	12	0.5	0.125	0.063
74	3.5	24	0.4	0.146	0.058
75	3.0	24	0.4	0.125	0.050
98	1.5	16	0.5	0.094	0.047
80	1.2	24	0.9	0.050	0.045
99	1.8	24	0.6	0.075	0.045
90	2.0	40	0.8	0.050	0.040
76	2.5	40	0.6	0.063	0.038
85	7.2	160	0.8	0.045	0.036
88	4.2	72	0.6	0.058	0.035
102	1.0	20	0.7	0.050	0.035
79	4.0	205	0.9	0.020	0.018
78	3.5	205	0.9	0.017	0.015
83	1.5	72	0.7	0.021	0.015
81	2.1	205	0.9	0.010	0.009

Table 33 Whole Set of Risks Sorted iaw Risk Prioritization Method 3

RISK NO	EXPOSURE	RISK MITIGATION COST (man-hour)	Prob. for Mitigation	Exposure/Risk Mitigation Cost	(Exposure * Probability for Mitigation) / Risk Mitigation Cost
73	5.4	12	0.7	0.450	0.315
55	2.4	8	0.8	0.300	0.240
69	5.4	20	0.8	0.270	0.216
82	2.0	8	0.8	0.250	0.200
1	5.6	16	0.5	0.350	0.175
94	5.4	16	0.5	0.338	0.169
70	5.4	27	0.8	0.200	0.160
57	3.5	16	0.6	0.219	0.131
49	3.5	16	0.6	0.219	0.131
72	2.0	16	0.9	0.125	0.113
95	3.5	16	0.5	0.219	0.109
97	3.5	16	0.5	0.219	0.109
62	3.5	16	0.5	0.219	0.109
93	3.5	16	0.5	0.219	0.109
101	5.6	32	0.6	0.175	0.105
92	4.0	24	0.6	0.167	0.100
58	4.9	40	0.8	0.123	0.098
60	4.9	40	0.8	0.123	0.098
10	4.2	40	0.9	0.105	0.095
4	3.0	16	0.5	0.188	0.094
56	3.0	16	0.5	0.188	0.094
100	3.0	16	0.5	0.188	0.094
23	2.8	16	0.5	0.175	0.088
77	4.2	20	0.8	0.105	0.084
29	2.1	8	0.3	0.263	0.079
64	2.5	16	0.5	0.156	0.078
96	2.4	16	0.5	0.150	0.075
15	4.2	40	0.7	0.105	0.074
87	4.9	48	0.7	0.102	0.071
91	2.1	16	0.5	0.131	0.066
86	3.5	32	0.6	0.109	0.066
84	2.0	16	0.5	0.125	0.063
89	1.5	12	0.5	0.125	0.063
68	0.6	8	0.8	0.075	0.060
25	5.4	64	0.7	0.084	0.059
74	3.5	24	0.4	0.146	0.058
50	1.8	16	0.5	0.113	0.056
45	2.4	40	0.9	0.060	0.054

Table 33 Whole Set of Risks Sorted iaw Risk Prioritization Method 3 (cont'd)

3	2.4	32	0.7	0.075	0.053
2	3.5	48	0.7	0.073	0.051
54	3.5	48	0.7	0.073	0.051
28	0.9	16	0.9	0.056	0.051
75	3.0	24	0.4	0.125	0.050
13	2.0	24	0.6	0.083	0.050
46	2.0	32	0.8	0.063	0.050
63	2.8	40	0.7	0.070	0.049
59	7.2	136	0.9	0.053	0.048
98	1.5	16	0.5	0.094	0.047
20	1.5	16	0.5	0.094	0.047
61	2.5	32	0.6	0.078	0.047
99	1.8	24	0.6	0.075	0.045
14	2.0	40	0.9	0.050	0.045
80	1.2	24	0.9	0.050	0.045
21	3.5	48	0.6	0.073	0.044
12	1.5	32	0.9	0.047	0.042
33	4.2	80	0.8	0.053	0.042
90	2.0	40	0.8	0.050	0.040
51	1.2	28	0.9	0.043	0.039
76	2.5	40	0.6	0.063	0.038
44	1.5	32	0.8	0.047	0.038
8	0.5	12	0.9	0.042	0.038
85	7.2	160	0.8	0.045	0.036
88	4.2	72	0.6	0.058	0.035
65	2.0	40	0.7	0.050	0.035
102	1.0	20	0.7	0.050	0.035
67	4.2	112	0.9	0.038	0.034
53	3.5	64	0.6	0.055	0.033
47	1.4	40	0.9	0.035	0.032
36	4.5	120	0.8	0.038	0.030
22	0.6	16	0.8	0.038	0.030
32	3.5	96	0.8	0.036	0.029
43	3.5	112	0.9	0.031	0.028
5	5.6	144	0.7	0.039	0.027
16	1.2	32	0.7	0.038	0.026
26	2.0	48	0.6	0.042	0.025
48	3.0	96	0.8	0.031	0.025
6	4.9	160	0.8	0.031	0.025
37	2.8	80	0.7	0.035	0.025
39	2.8	80	0.7	0.035	0.025
24	2.5	64	0.6	0.039	0.023
66	0.9	32	0.8	0.028	0.023
17	0.5	20	0.9	0.025	0.023

Table 33 Whole Set of Risks Sorted iaw Risk Prioritization Method 3 (cont'd)

34	2.0	64	0.7	0.031	0.022
71	0.9	40	0.9	0.023	0.020
19	3.0	120	0.8	0.025	0.020
35	1.5	72	0.9	0.021	0.019
38	2.1	80	0.7	0.026	0.018
7	1.8	80	0.8	0.023	0.018
79	4.0	205	0.9	0.020	0.018
9	3.5	120	0.6	0.029	0.018
30	1.5	64	0.6	0.023	0.016
78	3.5	205	0.9	0.017	0.015
31	3.0	160	0.8	0.019	0.015
27	0.6	32	0.8	0.019	0.015
83	1.5	72	0.7	0.021	0.015
41	1.5	64	0.7	0.023	0.014
52	1.5	64	0.6	0.023	0.014
18	1.2	72	0.8	0.017	0.013
42	1.2	96	0.8	0.013	0.010
11	2.4	200	0.8	0.012	0.010
81	2.1	205	0.9	0.010	0.009
40	0.6	72	0.6	0.008	0.005

APPENDIX D

DISTRIBUTION OF PRIORITIZED RISK ITEMS FOR EACH CLASS AND WHOLE SET IN ACCORDANCE WITH RISK PRIORITIZATION METHODS

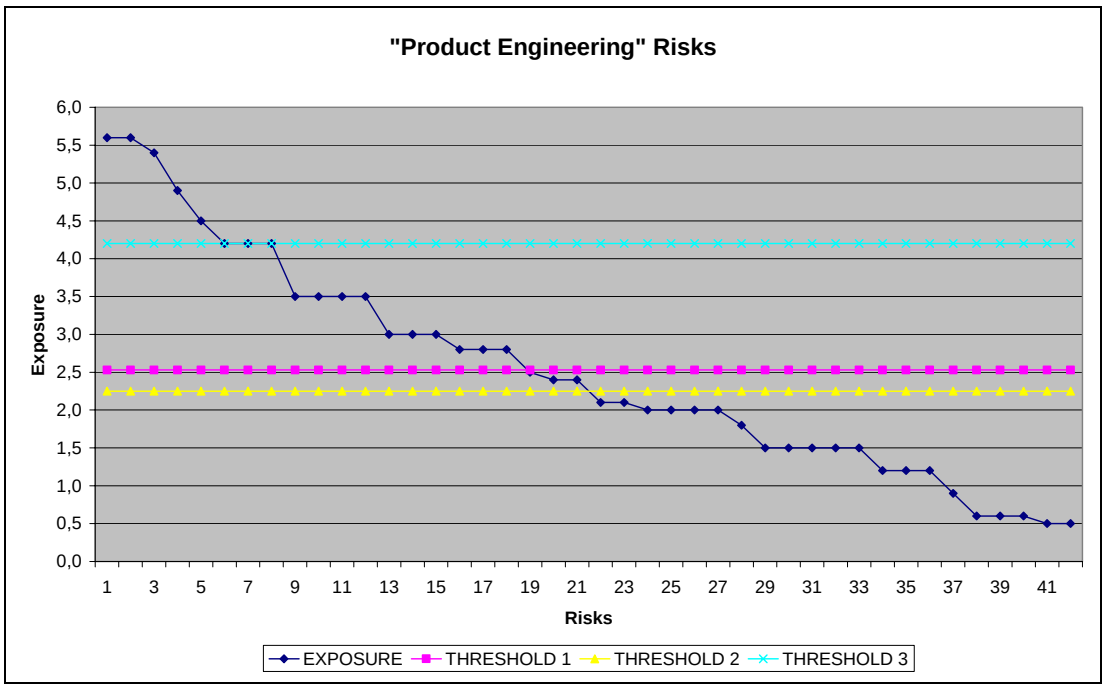

Figure 3 Exposure Values of 'Product Engineering' Risks iaw Risk Prioritization Method 1

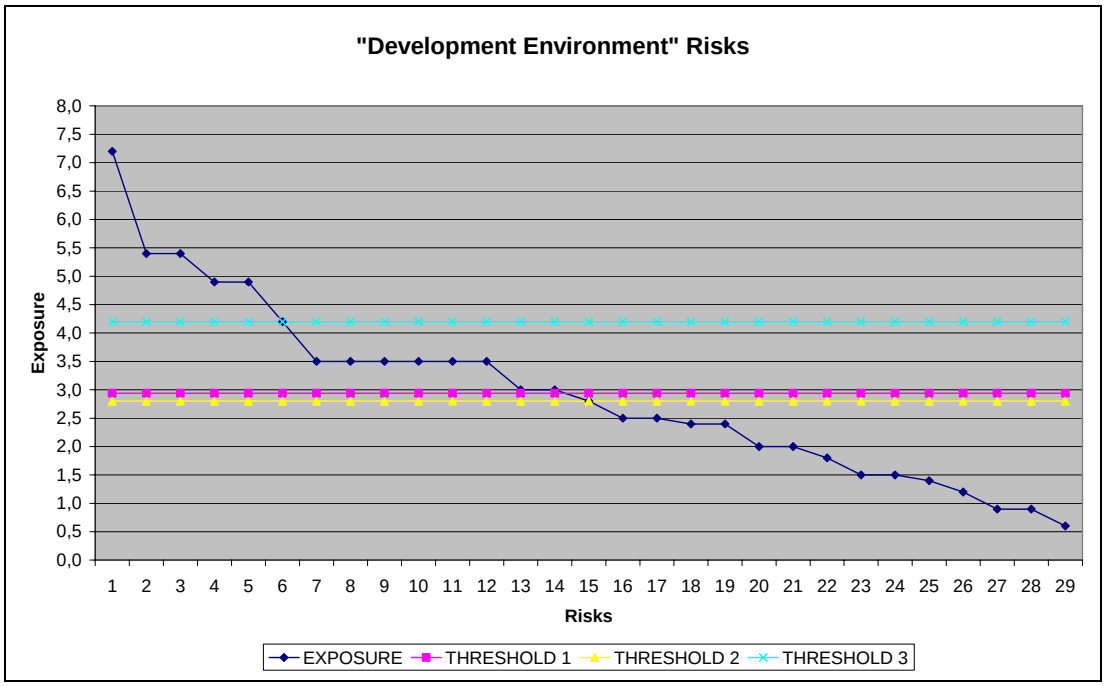

Figure 4 Exposure Values of 'Development Environment' Risks iaw Risk Prioritization Method 1

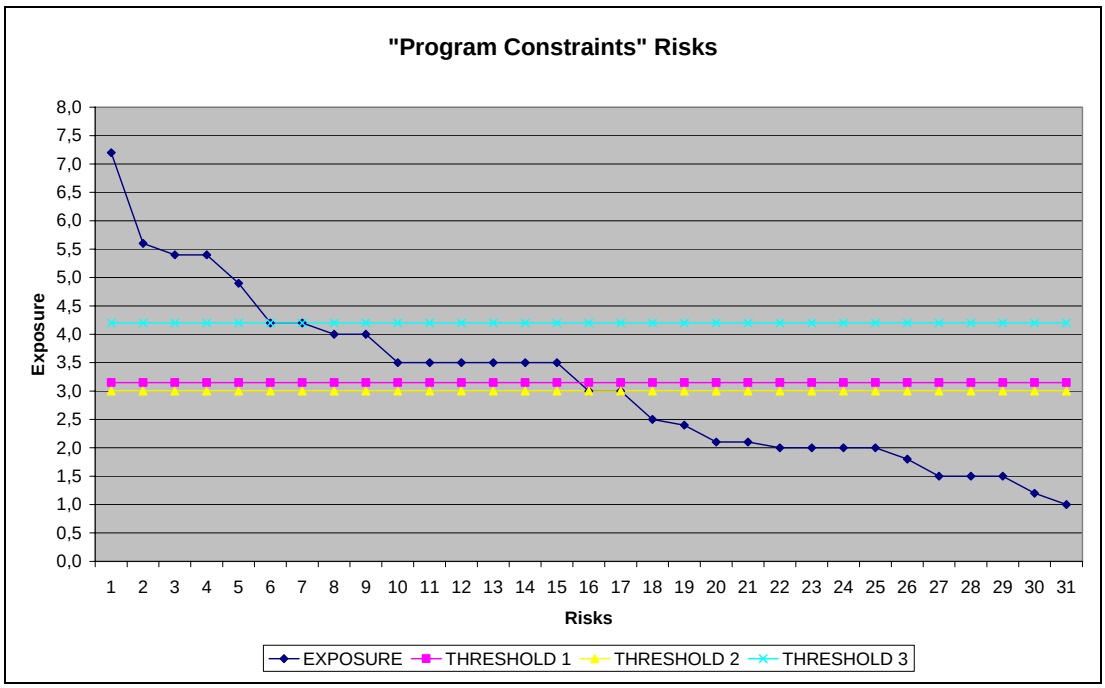

Figure 5 Exposure Values of 'Program Constraints' Risks iaw Risk Prioritization Method 1

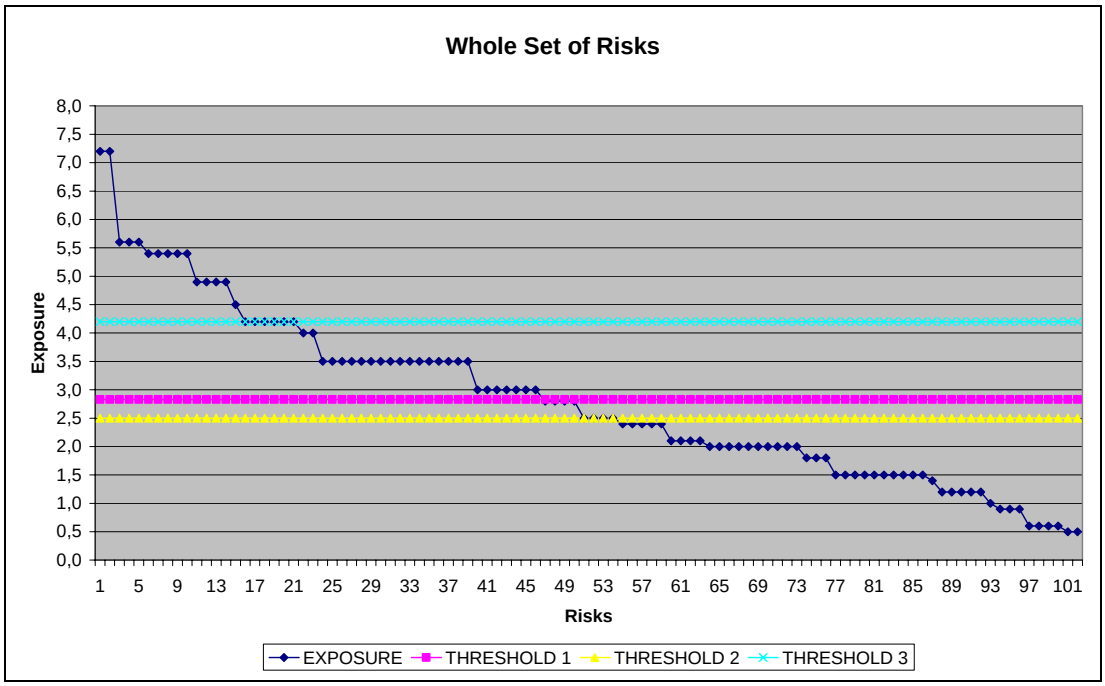

Figure 6 Exposure Values of Whole Set of Risks iaw Risk Prioritization Method 1

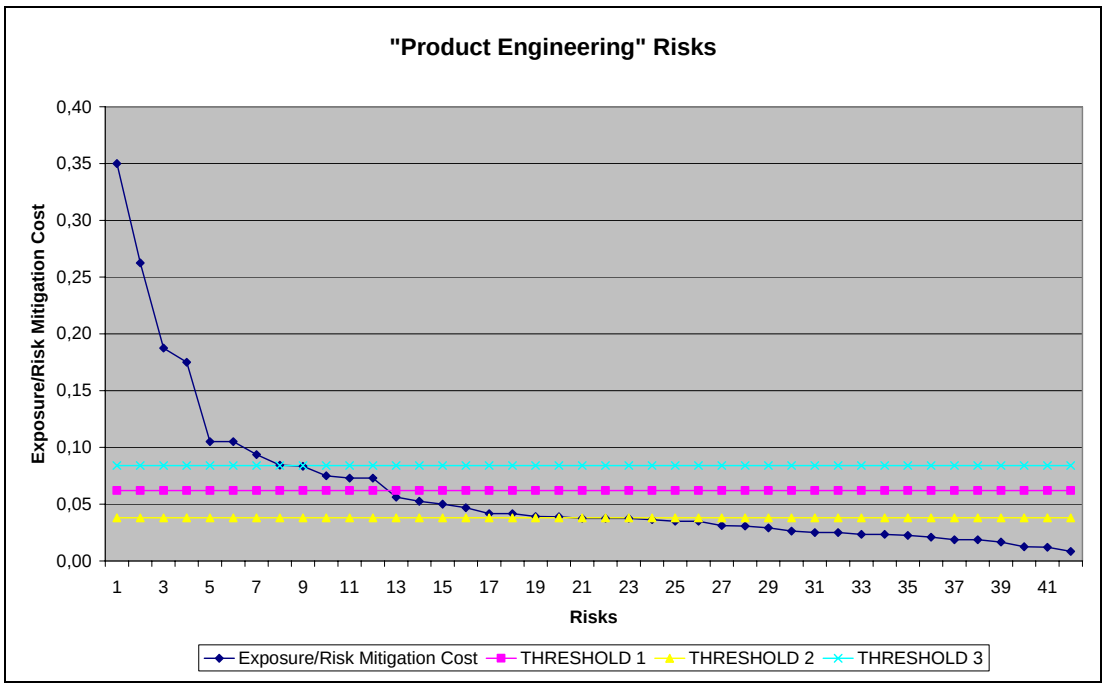

Figure 7 “Exposure/Risk Mitigation Cost” Values of ‘Product Engineering’ Risks iaw Risk Prioritization Method 2

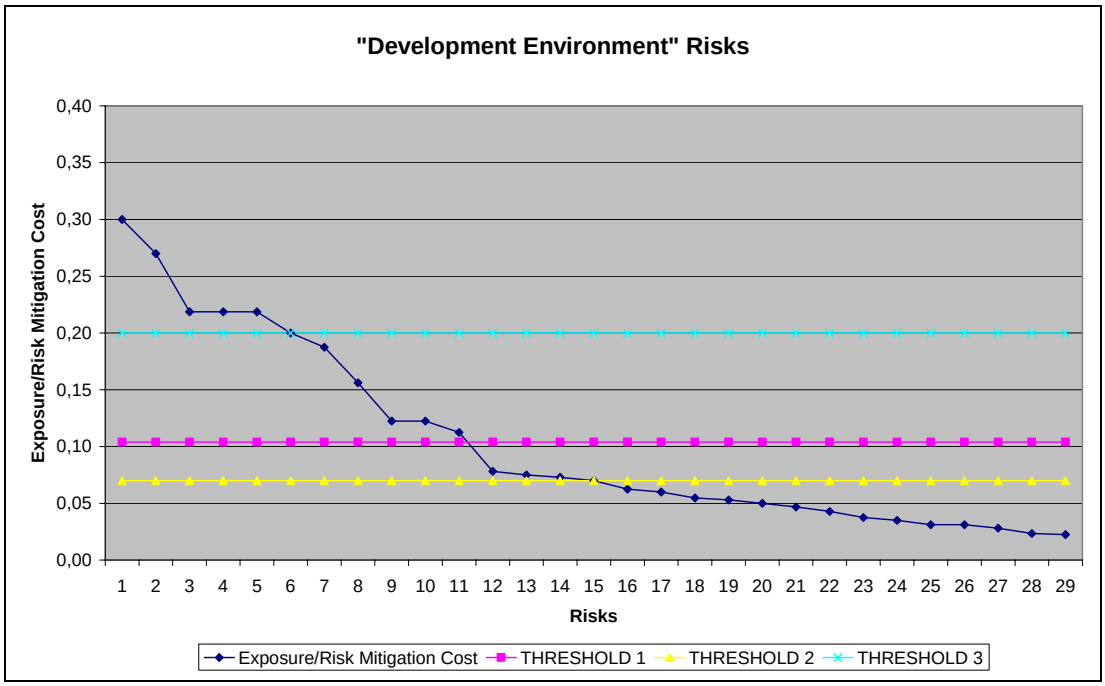

Figure 8 "Exposure/Risk Mitigation Cost" Values of 'Development Environment' Risks iaw Risk Prioritization Method 2

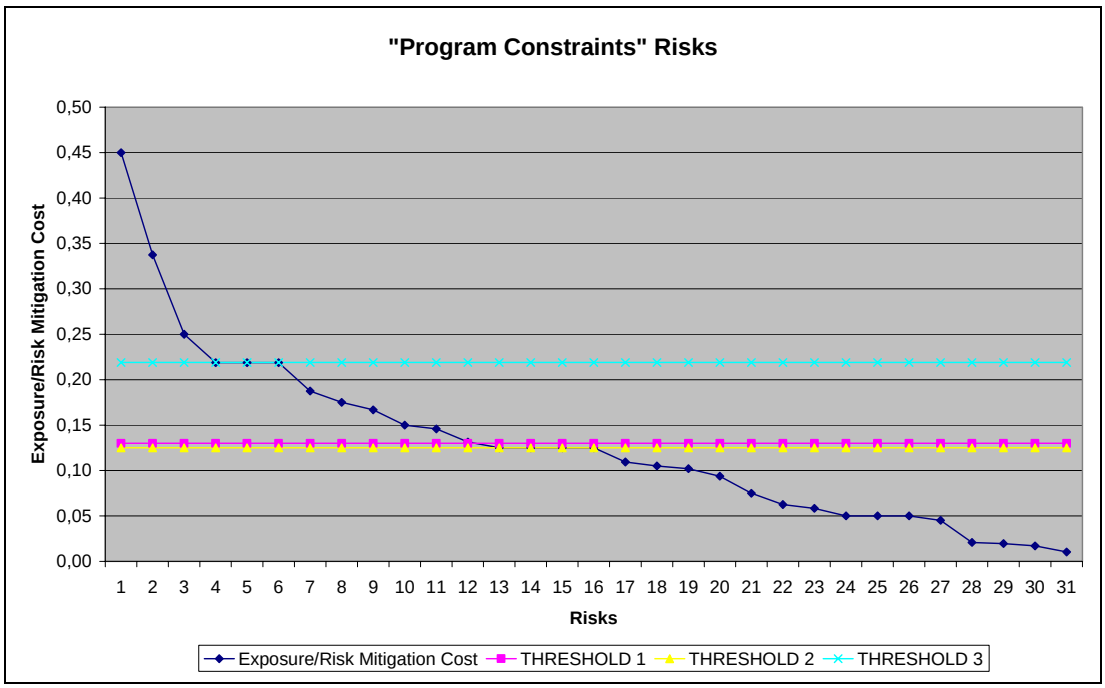

Figure 9 "Exposure/Risk Mitigation Cost" Values of 'Program Constraints' Risks iaw Risk Prioritization Method 2

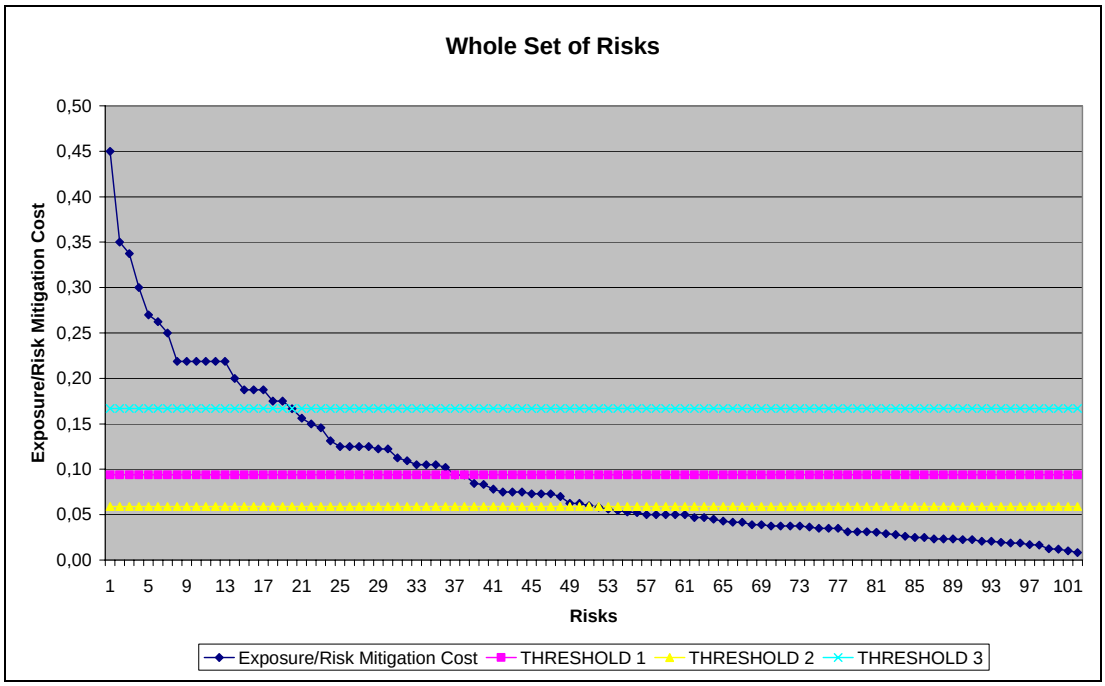

Figure 10 "Exposure/Risk Mitigation Cost" Values of Whole Set of Risks iaw Risk Prioritization Method 2

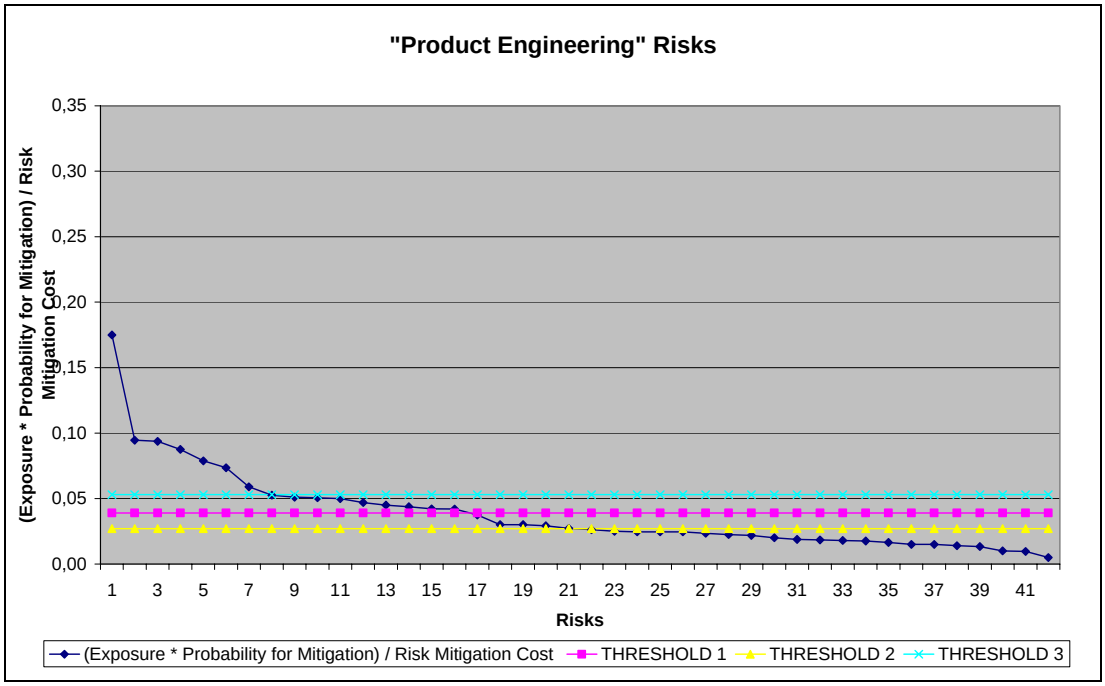

Figure 11 "Exposure * Probability for Mitigation / Risk Mitigation Cost" Values of 'Product Engineering' Risks iaw Risk Prioritization Method 3

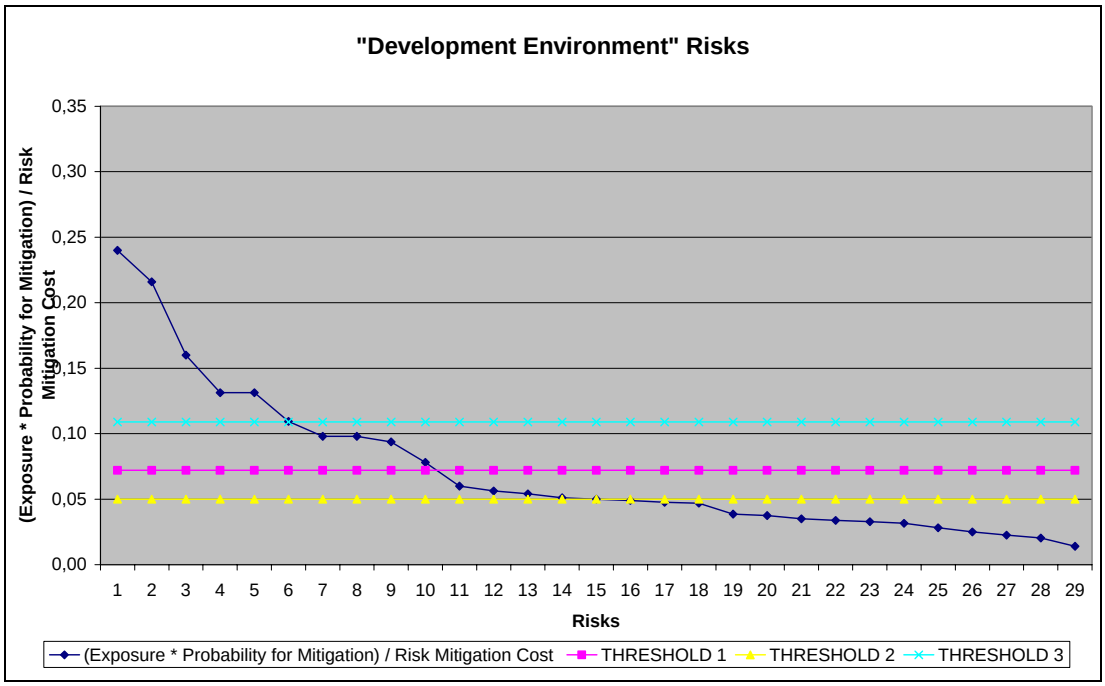

Figure 12 “Exposure * Probability for Mitigation / Risk Mitigation Cost” Values of ‘Development Environment’ Risks iaw Risk Prioritization Method 3

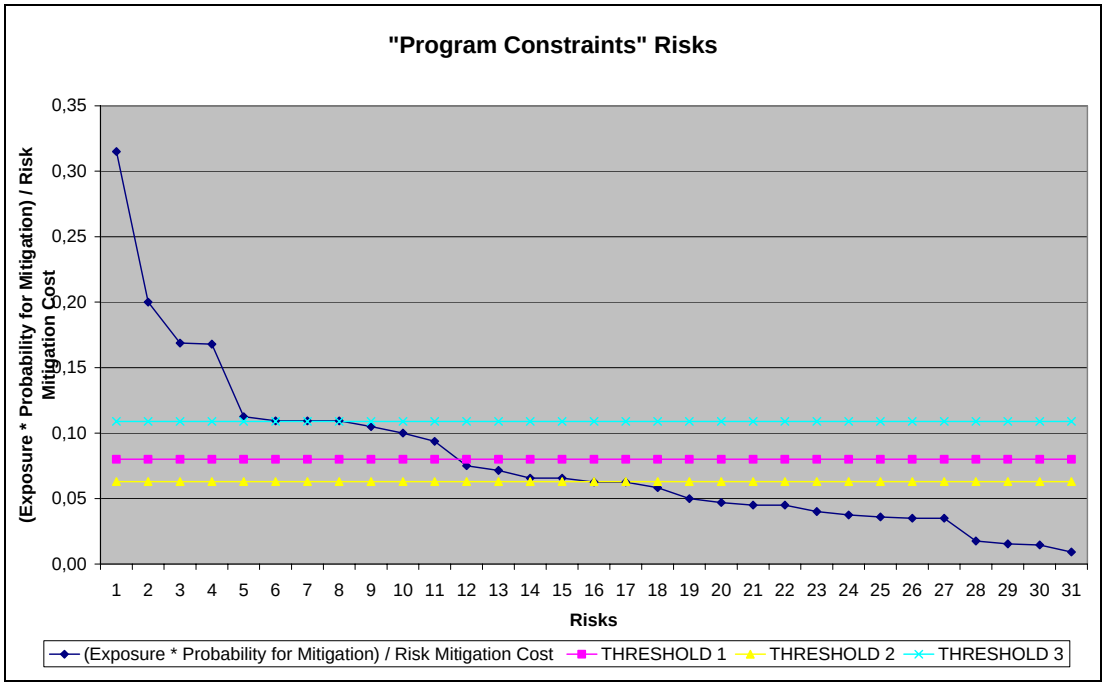

Figure 13 “Exposure * Probability for Mitigation / Risk Mitigation Cost” Values of ‘Program Constraints’ Risks iaw Risk Prioritization Method 3

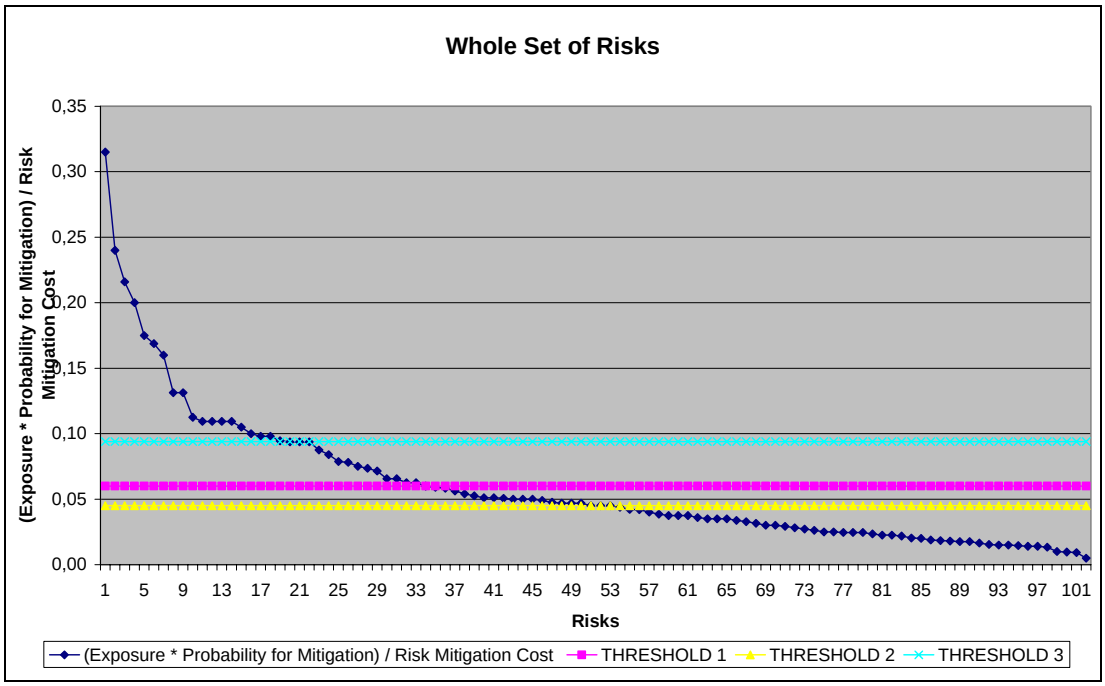

Figure 14 “Exposure * Probability for Mitigation / Risk Mitigation Cost” Values of Whole Set of Risks iaw Risk Prioritization Method 3

APPENDIX E

VALUES OF DECISION PARAMETERS FOR POLICIES

Table 34 Values of Decision Parameters for Policy 1&4

				Policy 1	**Policy 4**
Risk Prioritization Method 1 – Threshold 1	**Product Engineering Class**	**Development Environment Class**	**Program Constraints Class**	**Total**	**Whole Set**
Risk Items					
# of risk items mitigated	18	14	15	47	46
# of risk items monitored	24	15	16	55	56
percentage of risk items mitigated	0.43	0.48	0.48	0.46	0.45
Exposure					
total exposure prevented for mitigated risks	1.492	1.839	2.388	5.719	5.786

Table 34 Values of Decision Parameters for Policy 1&4 (cont'd)

total exposure released for monitored risks	1.106	1.163	1.631	3.900	3.833
percentage of total exposure prevented	0.57	0.61	0.59	0.59	0.60
Risk Mitigation Cost					
risk mitigation costs for mitigated risks (man-hour)	1448	759	898	3105	2989
potential risk mitigation costs for monitored risks (man-hour)	1256	468	565	2289	2425
percentage of risk mitigation costs	0.54	0.62	0.61	0.58	0.55
Probability for Mitigation					
total expected exposure prevented for mitigated risks	0.932	1.256	1.400	3.588	3.596
total expected exposure released for monitored risks	0.691	0.834	0.995	2.520	2.512
percentage of total expected exposure prevented	0.57	0.60	0.58	0.59	0.59
total exposure prevented for mitigated risks / # of risk items mitigated	0.083	0.131	0.159	0.122	0.126

Table 34 Values of Decision Parameters for Policy 1&4 (cont'd)

risk mitigation costs for mitigated risks / # of risk items mitigated	80.44	54.21	59.87	66.06	64.98
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.052	0.090	0.093	0.076	0.078
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	10.3 * 10-4	24.2 * 10-4	26.6 * 10-4	18.42 * 10-4	19.35 * 10-4
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	6.4 * 10-4	16.5 * 10-4	15.6 * 10-4	11.56 * 10-4	12.03 * 10-4

Table 35 Values of Decision Parameters for Policy 2&5

				Policy 2	**Policy 5**
Risk Prioritization Method 1 – Threshold 2	**Product Engineering Class**	**Development Environment Class**	**Program Constraints Class**	**Total**	**Whole Set**
Risk Items					
# of risk items mitigated	21	15	17	53	54
# of risk items monitored	21	14	14	49	48
percentage of risk items mitigated	0.50	0.52	0.55	0.52	0.53
Exposure					
total exposure prevented for mitigated risks	1.618	1.909	2.700	6.227	6.437
total exposure released for monitored risks	0.980	1.093	1.319	3.392	3.182
percentage of total exposure prevented	0.62	0.64	0.67	0.65	0.67
Risk Mitigation Cost					
risk mitigation costs for mitigated risks (man-hour)	1744	799	938	3481	3357
potential risk mitigation costs for monitored risks (man-hour)	960	428	525	1913	2057
percentage of risk mitigation costs	0.64	0.65	0.64	0.65	0.62

Table 35 Values of Decision Parameters for Policy 2&5 (cont'd)

Probability for Mitigation					
total expected exposure prevented for mitigated risks	1.018	1.305	1.544	3.867	3.967
total expected exposure released for monitored risks	0.605	0.785	0.851	2.241	2.141
percentage of total expected exposure prevented	0.63	0.62	0.64	0.63	0.65
total exposure prevented for mitigated risks / # of risk items mitigated	0.077	0.127	0.159	0.117	0.119
risk mitigation costs for mitigated risks / # of risk items mitigated	83.05	53.27	55.18	65.68	62.17
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.048	0.087	0.091	0.073	0.073
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$9.3 * 10^{-4}$	$23.9 * 10^{-4}$	$28.8 * 10^{-4}$	$17.89 * 10^{-4}$	$19.17 * 10^{-4}$
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$5.8 * 10^{-4}$	$16.3 * 10^{-4}$	$16.4 * 10^{-4}$	$11.11 * 10^{-4}$	$11.82 * 10^{-4}$

Table 36 Values of Decision Parameters for Policy 3&6

				Policy 3	**Policy 6**
Risk Prioritization Method 1 – Threshold 3	**Product Engineering Class**	**Development Environment Class**	**Program Constraints Class**	**Total**	**Whole Set**
Risk Items					
# of risk items mitigated	8	6	7	21	21
# of risk items monitored	34	23	24	81	81
percentage of risk items mitigated	0.19	0.21	0.23	0.21	0.21
Exposure					
total exposure prevented for mitigated risks	0.804	0.805	1.273	2.882	2.882
total exposure released for monitored risks	1.794	2.197	2.746	6.737	6.737
percentage of total exposure prevented	0.31	0.27	0.32	0.30	0.30
Risk Mitigation Cost					
risk mitigation costs for mitigated risks (man-hour)	664	375	360	1399	1399
potential risk mitigation costs for monitored risks (man-hour)	2040	852	1104	3996	3996
percentage of risk mitigation costs	0.25	0.31	0.25	0.26	0.26
Probability for Mitigation					

Table 36 Values of Decision Parameters for Policy 3&6 (cont'd)

total expected exposure prevented for mitigated risks	0.526	0.653	0.899	2.078	1.994
total expected exposure released for monitored risks	1.098	1.436	1.58	4.114	4.114
percentage of total expected exposure prevented	0.32	0.31	0.36	0.34	0.33
total exposure prevented for mitigated risks / # of risk items mitigated	0.101	0.134	0.182	0.137	0.137
risk mitigation costs for mitigated risks / # of risk items mitigated	83.00	62.50	51.43	66.62	66.62
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.066	0.109	0.128	0.099	0.095
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$12.1 * 10^{-4}$	$21.5 * 10^{-4}$	$35.4 * 10^{-4}$	$20.60 * 10^{-4}$	$20.60 * 10^{-4}$
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$7.9 * 10^{-4}$	$17.4 * 10^{-4}$	$25.0 * 10^{-4}$	$14.85 * 10^{-4}$	$14.25 * 10^{-4}$

Table 37 Values of Decision Parameters for Policy 7&10

				Policy 7	Policy 10
Risk Prioritization Method 2 – Threshold 1	**Product Engineering Class**	**Development Environment Class**	**Program Constraints Class**	**Total**	**Whole Set**
Risk Items					
# of risk items mitigated	12	11	12	35	38
# of risk items monitored	30	18	19	67	64
percentage of risk items mitigated	0.29	0.38	0.39	0.34	0.37
Exposure					
total exposure prevented for mitigated risks	1.667	2.128	2.650	6.445	6.966
total exposure released for monitored risks	0.930	0.875	1.369	3.174	2.652
percentage of total exposure prevented	0.64	0.71	0.66	0.67	0.72
Risk Mitigation Cost					
risk mitigation costs for mitigated risks (man-hour)	368	231	212	811	779
potential risk mitigation costs for monitored risks (man-hour)	2336	996	1252	4584	4616
percentage of risk mitigation costs	0.14	0.19	0.14	0.15	0.14
Probability for Mitigation					

Table 37 Values of Decision Parameters for Policy 7&10 (cont'd)

total expected exposure prevented for mitigated risks	0.906	1.412	1.510	3.828	4.127
total expected exposure released for monitored risks	0.717	0.678	0.886	2.281	1.982
percentage of total expected exposure prevented	0.56	0.68	0.63	0.63	0.68
total exposure prevented for mitigated risks / # of risk items mitigated	0.139	0.193	0.221	0.184	0.183
risk mitigation costs for mitigated risks / # of risk items mitigated	30.67	21.00	17.67	23.17	20.50
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.076	0.128	0.126	0.109	0.109
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$45.3 * 10^{-4}$	$92.1 * 10^{-4}$	$125.0 * 10^{-4}$	$79.47 * 10^{-4}$	$89.42 * 10^{-4}$
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$24.6 * 10^{-4}$	$61.1 * 10^{-4}$	$71.2 * 10^{-4}$	$47.20 * 10^{-4}$	$52.98 * 10^{-4}$

Table 38 Values of Decision Parameters for Policy 8&11

				Policy 8	**Policy 11**
Risk Prioritization Method 2 – Threshold 2	**Product Engineering Class**	**Development Environment Class**	**Program Constraints Class**	**Total**	**Whole Set**
Risk Items					
# of risk items mitigated	23	15	16	54	51
# of risk items monitored	19	14	15	48	51
percentage of risk items mitigated	0.55	0.52	0.52	0.53	0.50
Exposure					
total exposure prevented for mitigated risks	2.147	2.424	3.150	7.721	7.911
total exposure released for monitored risks	0.451	0.579	0.869	1.899	1.708
percentage of total exposure prevented	0.83	0.81	0.78	0.80	0.82
Risk Mitigation Cost					
risk mitigation costs for mitigated risks (man-hour)	972	359	280	1611	1259
potential risk mitigation costs for monitored risks (man-hour)	1732	868	1184	3784	4136
percentage of risk mitigation costs	0.36	0.29	0.19	0.30	0.23
Probability for Mitigation					

Table 38 Values of Decision Parameters for Policy 8&11 (cont'd)

total expected exposure prevented for mitigated risks	1.285	1.619	1.797	4.701	4.777
total expected exposure released for monitored risks	0.338	0.471	0.598	1.407	1.332
percentage of total expected exposure prevented	0.79	0.77	0.75	0.77	0.78
total exposure prevented for mitigated risks / # of risk items mitigated	0.093	0.162	0.197	0.143	0.155
risk mitigation costs for mitigated risks / # of risk items mitigated	42.26	23.93	17.50	29.83	24.69
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.056	0.108	0.112	0.087	0.094
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$22.1 * 10^{-4}$	$67.5 * 10^{-4}$	$112.5 * 10^{-4}$	$47.93 * 10^{-4}$	$62.84 * 10^{-4}$
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$13.2 * 10^{-4}$	$45.1 * 10^{-4}$	$64.2 * 10^{-4}$	$29.18 * 10^{-4}$	$37.94 * 10^{-4}$

Table 39 Values of Decision Parameters for Policy 9&12

				Policy 9	**Policy 12**
Risk Prioritization Method 2 – Threshold 3	**Product Engineering Class**	**Development Environment Class**	**Program Constraints Class**	**Total**	**Whole Set**
Risk Items					
# of risk items mitigated	8	6	6	20	20
# of risk items monitored	34	23	25	82	82
percentage of risk items mitigated	0.19	0.21	0.19	0.20	0.20
Exposure					
total exposure prevented for mitigated risks	1.363	1.426	1.694	4.483	4.812
total exposure released for monitored risks	1.235	1.576	2.325	5.136	4.807
percentage of total exposure prevented	0.52	0.48	0.42	0.47	0.50
Risk Mitigation Cost					
risk mitigation costs for mitigated risks (man-hour)	216	103	84	403	331
potential risk mitigation costs for monitored risks (man-hour)	2488	1124	1380	4992	5064
percentage of risk mitigation costs	0.08	0.08	0.06	0.07	0.06
Probability for Mitigation					

Table 39 Values of Decision Parameters for Policy 9&12 (cont'd)

total expected exposure prevented for mitigated risks	0.709	0.988	1.012	2.709	2.827
total expected exposure released for monitored risks	0.915	1.102	1.467	3.484	3.281
percentage of total expected exposure prevented	0.44	0.47	0.41	0.44	0.46
total exposure prevented for mitigated risks / # of risk items mitigated	0.170	0.238	0.282	0.224	0.241
risk mitigation costs for mitigated risks / # of risk items mitigated	27.00	17.17	14.00	20.15	16.55
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.089	0.165	0.169	0.135	0.141
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$63.1 * 10^{-4}$	$138.4 * 10^{-4}$	$201.7 * 10^{-4}$	$111.24 * 10^{-4}$	$145.38 * 10^{-4}$
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$32.8 * 10^{-4}$	$95.9 * 10^{-4}$	$120.5 * 10^{-4}$	$67.22 * 10^{-4}$	$85.41 * 10^{-4}$

Table 40 Values of Decision Parameters for Policy 13&16

				Policy 13	**Policy 16**
Risk Prioritization Method 3 – Threshold 1	**Product Engineering Class**	**Development Environment Class**	**Program Constraints Class**	**Total**	**Whole Set**
Risk Items					
# of risk items mitigated	16	10	11	37	34
# of risk items monitored	26	19	20	65	68
percentage of risk items mitigated	0.38	0.34	0.35	0.36	0.33
Exposure					
total exposure prevented for mitigated risks	1.873	2.015	2.453	6.341	6.471
total exposure released for monitored risks	0.725	0.987	1.566	3.278	3.148
percentage of total exposure prevented	0.72	0.67	0.61	0.66	0.67
Risk Mitigation Cost					
risk mitigation costs for mitigated risks (man-hour)	536	215	192	943	691
potential risk mitigation costs for monitored risks (man-hour)	2168	1012	1272	4452	4704
percentage of risk mitigation costs	0.20	0.18	0.13	0.17	0.13
Probability for Mitigation					

Table 40 Values of Decision Parameters for Policy 13&16 (cont'd)

total expected exposure prevented for mitigated risks	1.086	1.356	1.591	4.033	3.929
total expected exposure released for monitored risks	0.537	0.734	0.888	2.159	2.180
percentage of total expected exposure prevented	0.67	0.65	0.64	0.65	0.64
total exposure prevented for mitigated risks / # of risk items mitigated	0.117	0.202	0.223	0.171	0.190
risk mitigation costs for mitigated risks / # of risk items mitigated	33.50	21.50	17.45	25.49	20.32
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.068	0.136	0.145	0.109	0.116
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$34.9 * 10^{-4}$	$93.7 * 10^{-4}$	$127.8 * 10^{-4}$	$67.24 * 10^{-4}$	$93.65 * 10^{-4}$
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$20.3 * 10^{-4}$	$63.1 * 10^{-4}$	$82.9 * 10^{-4}$	$42.77 * 10^{-4}$	$56.86 * 10^{-4}$

Table 41 Values of Decision Parameters for Policy 14&17

				Policy 14	**Policy 17**
Risk Prioritization Method 3 – Threshold 2	**Product Engineering Class**	**Development Environment Class**	**Program Constraints Class**	**Total**	**Whole Set**
Risk Items					
# of risk items mitigated	21	15	17	53	53
# of risk items monitored	21	14	14	49	49
percentage of risk items mitigated	0.50	0.52	0.55	0.52	0.52
Exposure					
total exposure prevented for mitigated risks	2.065	2.398	3.196	7.659	7.985
total exposure released for monitored risks	0.533	0.605	0.823	1.961	1.634
percentage of total exposure prevented	0.79	0.80	0.80	0.80	0.83
Risk Mitigation Cost					
risk mitigation costs for mitigated risks (man-hour)	924	359	332	1615	1387
potential risk mitigation costs for monitored risks (man-hour)	1780	868	1132	3780	4008
percentage of risk mitigation costs	0.34	0.29	0.23	0.30	0.26
Probability for Mitigation					

Table 41 Values of Decision Parameters for Policy 14&17 (cont'd)

total expected exposure prevented for mitigated risks	1.240	1.627	1.994	4.861	4.884
total expected exposure released for monitored risks	0.384	0.463	0.485	1.332	1.225
percentage of total expected exposure prevented	0.76	0.78	0.80	0.78	0.80
total exposure prevented for mitigated risks / # of risk items mitigated	0.098	0.160	0.188	0.145	0.151
risk mitigation costs for mitigated risks / # of risk items mitigated	44.00	23.93	19.53	30.47	26.17
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.059	0.108	0.117	0.092	0.092
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$22.3 * 10^{-4}$	$66.8 * 10^{-4}$	$96.3 * 10^{-4}$	$47.42 * 10^{-4}$	$57.57 * 10^{-4}$
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$13.4 * 10^{-4}$	$45.3 * 10^{-4}$	$60.1 * 10^{-4}$	$30.10 * 10^{-4}$	$35.21 * 10^{-4}$

Table 42 Values of Decision Parameters for Policy 15&18

				Policy 15	**Policy 18**
Risk Prioritization Method 3 – Threshold 3	**Product Engineering Class**	**Development Environment Class**	**Program Constraints Class**	**Total**	**Whole Set**
Risk Items					
# of risk items mitigated	8	6	8	22	22
# of risk items monitored	34	23	23	80	80
percentage of risk items mitigated	0.19	0.21	0.26	0.22	0.22
Exposure					
total exposure prevented for mitigated risks	1.344	1.426	1.924	4.694	4.849
total exposure released for monitored risks	1.253	1.576	2.095	4.924	4.770
percentage of total exposure prevented	0.52	0.48	0.48	0.49	0.50
Risk Mitigation Cost					
risk mitigation costs for mitigated risks (man-hour)	232	103	120	455	443
potential risk mitigation costs for monitored risks (man-hour)	2472	1124	1344	4940	4952
percentage of risk mitigation costs	0.09	0.08	0.08	0.08	0.08
Probability for Mitigation					

Table 42 Values of Decision Parameters for Policy 15&18 (cont'd)

total expected exposure prevented for mitigated risks	0.715	0.988	1.292	2.995	3.064
total expected exposure released for monitored risks	0.909	1.102	1.187	3.198	3.044
percentage of total expected exposure prevented	0.44	0.47	0.52	0.48	0.50
total exposure prevented for mitigated risks / # of risk items mitigated	0.168	0.238	0.241	0.213	0.220
risk mitigation costs for mitigated risks / # of risk items mitigated	29.00	17.17	15.00	20.68	20.14
total expected exposure prevented for mitigated risks / # of risk items mitigated	0.089	0.165	0.162	0.136	0.139
total exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$57.9 * 10^{-4}$	$138.4 * 10^{-4}$	$160.3 * 10^{-4}$	$103.16 * 10^{-4}$	$109.46 * 10^{-4}$
total expected exposure prevented for mitigated risks / risk mitigation costs for mitigated risks	$30.8 * 10^{-4}$	$95.9 * 10^{-4}$	$107.7 * 10^{-4}$	$65.82 * 10^{-4}$	$69.16 * 10^{-4}$