GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.080

L 77

GB/T 20918-2007

Information technology – Software life cycle processes – Risk management

信息技术　软件生存周期过程　风险管理

Issued on: April 30, 2007 **Implemented on: July 1, 2007**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China;

Standardization Administration of the People's Republic of China.

Table of Contents

Information technology – Software life cycle processes – Risk management

1 Scope

1.1 Purpose

This standard describes a process for the management of risk during software acquisition, supply, development, operations, and maintenance. It is intended that both technical and managerial personnel throughout an organization apply this standard.

The purpose of this standard is to provide software suppliers, acquirers, developers, and managers with a single set of process requirements suitable for the management of a broad variety of risks. This standard does not provide detailed risk management techniques, but instead focuses on defining a process for risk management in which any of several techniques may be applied.

1.2 Field of application

This standard defines a process for the management of risk throughout the software life cycle. It is suitable for adoption by an organization for application to all appropriate projects or for use in an individual project. Although the standard is written for the management of risk in software projects, it may also be useful for the management of both system-level and organization-level risks.

This standard is written so that it may be applied in conjunction with GB/T 8566 or applied independently.

1.2.1 Application with GB/T 8566

GB/T 8566 describe standard processes for the acquisition, supply, development, operations, and maintenance of software. The standard recognizes that actively managing risk is a key success factor in the management of a software project. GB/T 8566 mentions risk and risk management in several places, but does not provide a process for risk management. This risk management standard provides that process. This standard may be used for managing organizational-level risk or project-level risk, in any domain or life cycle phase, to support the perspectives of managers, participants, and other stakeholders.

In the life cycle process framework provided by GB/T 8566, risk management is an “organizational life cycle process.” The activities and tasks in an organizational process are the responsibility of the organization using that process. The organization therefore

NOTE 1: ISO 3534-1:1993, definition 1.1, gives the mathematical definition of probability as “a real number in the scale 0 to 1 attached to a random event. It can be related to a long-run relative frequency of occurrence or to a degree of belief that an event will occur. For a high degree of belief, the probability is near 1.”

NOTE 2: Frequency rather than probability may be used in describing risk.

NOTE 3: Degrees of belief about probability can be chosen as classes or ranks, such as

- rare/unlikely/moderate/likely/almost certain, or

- incredible/improbable/remote/occasional/probable/frequent.

3.5

project risk profile

A project's current and historical risk-related information; a compendium or aggregate of all of the individual risk profiles in a project.

NOTE: The project risk profile information includes the risk management context, along with the chronological record of risks and their individual risk profiles, priority ordering, risk-related measures, treatment status, contingency plans, and risk action requests. A project risk profile consists of a collection of the risk profiles of all the individual risks, which in turn includes the current and historical risk states. See risk profile and risk state.

3.6

risk

The combination of the probability of an event and its consequence.

NOTE 1: The term “risk” is generally used only when there is at least the possibility of negative consequences.

NOTE 2: In some situations, risk arises from the possibility of deviation from the expected outcome or event.

NOTE 3: See ISO/IEC Guide 51 for issues related to safety.

3.7

risk acceptance

The decision to accept a risk.

NOTE: Risk acceptance depends on risk criteria.

risk throughout the life cycle of a product or service.

3.14

risk management system

Set of elements of an organization's management system concerned with managing risk.

NOTE 1: Management system elements can include strategic planning, decision making, and other processes for dealing with risk.

NOTE 2: The culture of an organization is reflected in its risk management system.

3.15

risk profile

A chronological record of a risk's current and historical risk state information.

3.16

risk state

The current project risk information relating to an individual risk.

NOTE: The information concerning an individual risk may include the current description, causes, probability, consequences, estimation scales, confidence of the estimates, treatment, threshold, and an estimate of when the risk will reach its threshold.

3.17

risk threshold

A condition that triggers some stakeholder action.

NOTE: Different risk thresholds may be defined for each risk, risk category or combination of risks based upon differing risk criteria.

3.18

risk treatment

The process of selection and implementation of measures to modify risk.

NOTE 1: The term "risk treatment" is sometimes used for the measures themselves.

NOTE 2: Risk treatment measures can include avoiding, optimizing, transferring or retaining risk.

be integrated and coordinated with an organization's problem management approaches, e.g., in the event that a contingency plan must be implemented. The risk treatment activity should be managed in the same manner as other project management activities.

5 Risk management in the software life cycle

5.0 Purpose of risk management

The purpose of the risk management is to identify and mitigate the risks continuously. As a result of successful implementation of risk management:

a) The scope of risk management to be performed will be determined.

b) Appropriate risk management strategies will be defined and implemented.

c) Risks will be identified in a strategy and as they develop during the conduct of the project.

d) The risks will be analyzed, and the priority in which to apply resources to monitor these risks will be determined.

e) Risk measures will be defined, applied, and assessed to determine changes in the status of risk and the progress of the monitoring activities.

f) Appropriate action will be taken to reduce or avoid the impact of risk.

5.1 Risk management process

The risk management process is a continuous process for systematically addressing risk throughout the life cycle of a product or service.

This process consists of the following activities:

a) Plan and implement risk management;

b) Manage the project risk profile;

c) Perform risk analysis;

d) Perform risk monitoring;

e) Perform risk treatment;

f) Evaluate the risk management process.

The risk management process is illustrated in Figure 1. Note that the performance of

The project risk profile information is continually updated and maintained through the "perform risk analysis" activity ④, which identifies the risks, determines their likelihood and consequences, determines their risk exposures, and prepares risk action requests recommending treatment for risks determined to be above their risk threshold(s).

Treatment recommendations, along with the status of other risks and their treatment status, are sent to management for review ⑤. Management decides what risk treatment is implemented for any risk found to be unacceptable. Risk treatment plans are created for risks that require treatment. These plans are coordinated with other management plans and other ongoing activities.

All risks are continually monitored until they no longer need to be tracked during the "perform risk monitoring" activity ⑥. In addition, new risks and sources are sought out.

Periodic evaluation of the risk management process is required to ensure its effectiveness. During the "evaluate the risk management process" activity ⑦, information, including user and other feedback, is captured for improving the process or for improving the organization's or project's ability to manage risk. Improvements defined as a result of evaluation are implemented in the "plan and implement risk management" activity ②.

The software risk management process is applied continuously throughout the product life cycle. However, activities and tasks of the risk management process interact with the individual risks in an iterative manner once the risk management process begins. For example, in the perform risk analysis activity ④, a risk may be re-estimated several times during the performance of risk evaluation due to an increase in knowledge about the risk gained during the evaluation task itself. The risk management process is not a "waterfall" process.

5.1.1 Plan and implement risk management

The purpose of the "plan and implement risk management" activity is to establish a software risk management process. Where an organizational risk management process exists, the software risk management process should be aligned to it. This activity shall establish who is to perform risk management, define the specific risk management process to be used, assign the resources required to implement the process, and define how risks and their treatment are to be communicated and coordinated among stakeholders.

This activity should be performed at the beginning of the project. Information created during this activity shall be documented in a risk management plan such as that found in Annex A.

NOTE: IEEE Std 1058-1998 requires the documentation of a risk management plan in the software project management plan.

g) Which stakeholder(s) perspectives the risk management process supports;

h) The risk categories to be considered.

During this task, risk management process, specific procedures, and techniques should be selected to match the project situation.

NOTE: IEC Guide 60300-3-9:1995 provides guidelines for the selection and utilization of commonly used risk analysis techniques. IEC Std 61508-7:2000 provides useful material related to measures and techniques related to safety.

The risk management process should align to existing organizational risk management processes whenever feasible. A documented organizational risk management process that defines the previous list may be referenced and only the specifics for a project need to be documented.

5.1.1.3 Establish responsibility

The parties responsible for performing risk management and their roles and responsibilities shall be explicitly identified. Parties shall be assigned responsibility for the risk management process within the organizational unit.

5.1.1.4 Assign resources

The responsible parties shall be provided with adequate resources to perform the risk management process.

5.1.1.5 Establish the risk management process evaluation

A description of the process for evaluating and improving the risk management process, along with how information will be captured for lessons learned, shall be provided. Any relevant lessons from prior use of the process should be incorporated into this implementation of the process.

5.1.2 Manage the project risk profile

The purpose of the “manage the project risk profile” activity is to create a consistent current and historical view of the risks present along with their treatment, so that the risks can be communicated fully and succinctly to relevant stakeholders. It includes the risk management context, the current risk state, and risk history.

The project risk profile shall be maintained throughout the life cycle.

This activity consists of the tasks listed in 5.1.2.1 through 5.1.2.4.

5.1.2.1 Define the risk management context

shall consist of, at a minimum,

a) The risk management context;

b) A chronological record of each risk's state including their probability, consequences, and risk thresholds;

c) The priority of each risk based on risk criteria supplied by the stakeholders;

d) The risk action requests for risks along with the status of their treatment.

The project risk profile should contain a detailed description of each risk, its causes, the estimation scales used, the risk-related measures used to evaluate status, contingency plans, and other risk-related information captured in the risk state.

The project risk profile shall be updated when there are changes in an individual risk's state, e.g., its description, exposure or treatment, changes occur to the risk management context, or a new risk is identified. Information should be captured in electronic form to ease its capture, communication, and assessment.

5.1.2.4 Communicate risk status

The project risk profile or relevant risk profile (e.g., a single or combination of risks) shall be communicated periodically to stakeholders based upon their needs. Risk status information should be made available as widely as possible to all the stakeholders.

5.1.3 Perform risk analysis

The purposes of the “perform risk analysis” activity are to:

a) Identify the initiating events, hazards, threats, or situations that create risks;

b) Estimate the probability of occurrence, the consequences for each risk, and the expected timing of the risk;

c) Evaluate each risk or defined combination of risks against its applicable threshold, generate alternatives to treat risks above their risk thresholds, and make recommendations for treatment based on a priority order.

Risk analysis shall be performed continuously throughout the life cycle.

The “perform risk analysis” activity consists of the tasks listed in 5.1.3.1 through 5.1.3.3.

5.1.3.1 Risk identification

Risks shall be identified in the categories included in the risk management context. Changes in the risk management context, e.g., additional risk due to changes in the

Various treatment alternatives to addressing risk should be considered to reduce or eliminate risks. For each risk that is above its risk threshold, recommended treatment strategies such as eliminating the risk, reducing its probability of occurrence or severity of consequence, or accepting the risk shall be defined and documented in a risk action request such as that found in Annex B. Contingency plans should be developed for all risks above their thresholds. Measures indicating the effectiveness of the treatment alternatives shall also be defined. The risks, their recommended treatments, and measures of risk treatment effectiveness shall be communicated to the stakeholders for approval, rejection, or modification.

NOTE: IEEE Std 982.1-1988 provides information that may be useful in defining risk-related measures. IEC 60300-3-9:1995, IEC Std 60812:1985 and IEC Std 61025:1990 provide useful techniques to aid in risk evaluation.

5.1.4 Perform risk treatment

The purposes of the “perform risk treatment” activity are to:

a) Determine whether risks are acceptable to the stakeholders, and if not,

b) Initiate actions to reduce the risks to an acceptable level.

Risk treatment involves the selection, planning, monitoring, and controlling of actions to decrease risk exposure.

Stakeholders shall evaluate for treatment every risk that is above its risk threshold. Risk treatment shall be continuously performed as required.

This activity consists of the tasks listed in 5.1.4.1 ~ 5.1.4.2.

5.1.4.1 Selecting risk treatment

Stakeholders shall be provided recommended alternatives for risk treatment in risk action requests. Whenever a risk treatment alternative is recommended in a risk action request, an evaluation shall be made by the stakeholders to determine if the risk is acceptable. If the stakeholders determine that actions should be taken to make a risk acceptable, then a risk treatment alternative shall be implemented, supported by the necessary resources, and monitored and coordinated with other project activities.

The stakeholders may accept a risk even though it exceeds its risk threshold, e.g., if the treatment cost is too high, the timing isn't suitable, or a lack of treatment resources exists. In this situation, the risk shall be considered a high priority and monitored continuously to determine if any future risk treatment actions are necessary.

The stakeholders may also ask that more information upon which to make a risk treatment decision be provided in the risk action request or they may suggest some

This activity consists of the tasks listed in 5.1.5.1 ~ 5.1.5.3.

5.1.5.1 Monitor risk

All risks shall be monitored throughout the life cycle for changes in their state using measures that will be recorded in the project risk profile. The risk management context shall also be monitored for changes and be documented in the project risk profile. Risks shall be placed in a monitoring priority order based on criteria supplied by the stakeholders (e.g., risk exposure, timing.). The monitoring priority should be reviewed periodically to verify that the priority ordering is still valid. High priority risks should be monitored frequently. Risks whose state has changed shall undergo risk evaluation. Evaluation should occur promptly after discovery.

5.1.5.2 Monitor risk treatment

Measures shall be implemented and monitored to evaluate the effectiveness of risk treatments. The cause of an ineffective treatment should be identified and remedied promptly. Criteria should be set by the stakeholders to determine when a risk no longer needs to be monitored for treatment effectiveness.

5.1.5.3 Seek new risks

The system shall be continuously monitored for new risks and sources throughout its life cycle. New risks and sources shall be communicated to the stakeholders after risk analysis.

5.1.6 Evaluate the risk management process

The purposes of the “evaluate the risk management process” activity are to provide feedback to the stakeholders regarding:

a) The quality of the risk management process;

b) Areas where the risk management procedures, process, or policies should be improved;

c) The identification of opportunities for modifying organizational risk management procedures, processes, or policies to better reduce or eliminate systemic risks.

This activity consists of the tasks listed in 5.1.6.1 through 5.1.6.3.

5.1.6.1 Capture risk management information

Information about the risks identified, their sources, their causes, their treatment, and the success of the treatments selected shall be collected throughout the project's life cycle for purposes of improving the risk management process and generating lessons learned. The information captured may be useful to improving organizational risk

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------