ISD Software Risk Identification

Number: 580-SP-013-001
Effective Date: September 1, 2004
Expiration Date: September 1, 2009

Approved By: (signature)
Name: Joe Hennessy
Title: Chief, ISD

Responsible Office: 580/Information Systems Division (ISD)
Title: Software Risk Identification

Asset Type: Sub-process
PAL Number: 1.2.3

Purpose

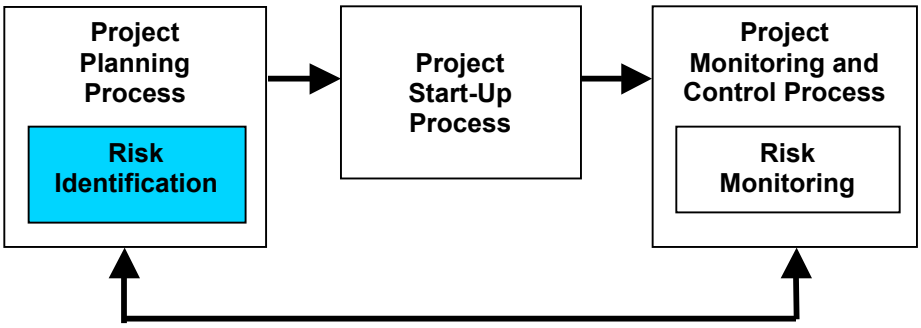
The purpose of Risk Identification is to identify potential threats to the success of the project before they occur, so that risk-handling activities may be planned and invoked as needed across the life cycle to avoid or mitigate adverse impacts to the project.

Scope

This sub-process applies to the initial risk identification performed during Project Planning, and to the subsequent identification of new risks as they arise. This sub-process is to be followed on all Information Systems Division (ISD) mission software development projects. This sub-process operates within the Project Planning process, and occasionally receives information from the Project Monitoring and Control process.

Context Diagram

Software Risk Identification



Check the Process Asset Library at http://software.gsfc.nasa.gov/process.cfm to obtain the latest version.
NOTE: Words or phrases shown in blue underlined contain links to additional information.
Guidance & tailoring information is shown in *italics with gray background*.

Roles and Responsibilities

Product Development Lead (PDL):

- Identify and analyze potential threats.
- Identify generic and project-specific risks.
- Document identified risks.
- Prepare the Risk Management Plan.
- Periodically identify new risks that occur during the project life cycle.

Development Team Leads (If applicable)

- Support the PDL in monitoring and controlling risks

  GUIDANCE: Development Team Leads are used on large software projects. Team Leads manage subsystems and report to the PDL.

Product Development Team Members:

- Support the Product Development Lead (PDL) in identifying risks.

GSFC Division Chief and/or Branch Head and/or Project Manager:

- Review and approve the Risk Management Plan.
- Conduct management reviews, including assessment of risks.

Usage Scenarios

This process is entered from the Project Planning Process. There are two usage scenarios:

- Initial entry at inception of the software development or maintenance project.
- Subsequent re-entry whenever new risks materialize.

GUIDANCE: Risk identification should occur at regularly scheduled intervals. It should also be performed whenever there is a significant change in the project circumstances that could result in new risks. Criteria that often trigger identification of new risks include:

- *Significant changes in scope/requirements, schedule, or budget*
- *Completion of a major phase of the software project (e.g., design)*
- *New project-specific risks that become evident as the project evolves. .*

When only very high-level requirements (e.g., an approved research proposal) are available for initial planning, partial risk identification may be performed. Additional risks may then be identified later as requirements, constraints, and resources are defined.

Inputs

- List of generic risks, developed from previous projects (if available)
- Budget and schedule estimates
- Project-level requirements from System Concept or Requirements Review
- Software system concept and architecture definition for current project
- (For reentry) Project Monitoring and Control risk information or events.

GUIDANCE: Risk identification should include both generic risks that exist across the organization and project-specific risks. An initial set of project-specific risks can be developed by examining software concept and architecture documentation that covers details of the planned software system and its dependencies (high-level concepts and requirements, software system architecture, schedule constraints, etc.) As the project evolves, additional project-specific risks will generally become evident. This process will be reentered periodically to address identification of new risks; relevant inputs will generally be project events rather than documents.

Entry Criteria

- (For initial entry) [All inputs are available
- Project Planning has begun]

OR (for re-entry)

- [Project Monitoring and Control has begun
- There are new risks to be identified
- Inputs are available.]

Exit Criteria

- Identified risks, with exposures and mitigation and/or contingency strategies, have been entered in approved Risk Management Plan and Database
- (If part of a Project) Risks have been reported to Project Management
- Appropriate approved risks have been submitted for addition to the generic risk set.

Outputs

- Risk Management Plan (which may be included in the SMP/PP)
- Risk Management Database
- Approved risks for addition to the generic risk set.

Major Tasks

The following major tasks are normally executed sequentially:

1. Identify risks. (PDL)
2. Estimate impact and likelihood of occurrence for each risk; combine these to estimate risk exposure. (PDL)
3. Classify risks. (PDL)
4. Develop the steps of a mitigation and/or contingency strategy for each high-exposure risk. (PDL)
5. Document initial identified risks and strategies in the Risk Management Plan. (PDL)
6. Record all identified risks in the Risk Management Database. (PDL)
7. Approve Risk Management Plan. (GSFC Project Manager and/or

Check the Process Asset Library at http://software.gsfc.nasa.gov/process.cfm to obtain the latest version.
NOTE: Words or phrases shown in blue underlined contain links to additional information.
Guidance & tailoring information is shown in *italics with gray background*.

Branch Chief and/or Division Chief)

8. Report risks to Project management or enter agreed-to risks into a Project-level risk tool. (PDL, reporting to Project Manager, and possibly to Branch Head and Division Chief)

GUIDANCE: The PDL has primary responsibility for carrying out risk identification. The Product Development Team members and, if applicable, the Development Team Leads have secondary responsibility and support the PDL in each of the Major Tasks.

Task 1: **Identify risks.** (**PDL**)

a) Develop a list of credible project-specific risks. These should include technical risks, budget and schedule risks, management risks, etc.

b) Discuss each identified risk with the Product Development Team (and with other stakeholders if necessary), and reach agreement on its applicability. Add each applicable risk to the risk set for the project.

c) Also consider each of the known generic risks that have been identified for the organization.

d) Determine whether the generic risk applies to the current project. If so, add it to the risk set for the project.

GUIDANCE: Each ISD Branch should consider maintaining its own list of generic software risks. .

Task 2: **Estimate impact and likelihood of occurrence for each risk; combine these to estimate risk exposure. (PDL)**

Guidance: Typically, impact and likelihood are each estimated on a multi-point scale, and then combined to determine the exposure of the risk. Sometimes the impact and likelihood are expressed numerically, and then multiplied to compute the risk exposure. Tabular representation can be helpful. A five-by-five table is most often used, although some NASA projects use four-by-five or four-by-four tables. The corner of the table that represents highest impact and greatest likelihood indicates the risks with highest exposure. See, for example, NPR 8000.4, "Risk Management Procedural Requirements."

Task 3: **Classify risks. (PDL)**

Review each risk in the risk set, whether project-specific or generic. Classify each risk according to its:

a) Estimated likelihood of occurrence

b) Estimated impact, should the risk occur

c) Exposure (i.e., combination of likelihood and impact)

d) Likely timeframe

e) Risk source (e.g., requirements, design, schedule, technology, staffing, cost, vendor, subcontractor, etc.)

f) Risk category (e.g., application domain, program management risks

Check the Process Asset Library at http://software.gsfc.nasa.gov/process.cfm to obtain the latest version.
NOTE: Words or phrases shown in blue underlined contain links to additional information.
Guidance & tailoring information is shown in *italics with gray background*.

[contract, budget, schedule, resource, performance, etc.], risks associated with a specific life-cycle phase [requirements, design, development, test, operations, maintenance, etc.], process risks, product risks [e.g., COTS/GOTS or other products required], etc.)

g) Initial status (e.g., identified, mitigation strategy developed, action taken, closed)

h) If the risk could be applicable to future projects, submit it as a candidate for inclusion in the generic risk set.

Guidance: Classification involves grouping risks based on common factors. This helps to identify duplicate or related risks, and can enable you to shorten and simplify the project risk set.

Task 4:

Develop the steps of a mitigation and/or contingency strategy for each high-exposure risk. (PDL)

a) Review each high-exposure risk, and the classification that was assigned to it during Task 3.

b) Determine whether actions can be taken to decrease the likelihood that the risk will occur, or to mitigate the effect of the risk.

c) Determine what contingency actions should be taken in the event that the risk materializes.

d) Identify the resources that will be required to support risk mitigation or carry out contingency actions.

e) If possible, define the steps of the mitigation and/or contingency strategy for the risk, and assign responsibility for each step.

Guidance: Part of the mitigation strategy is to estimate the probable cost of the risk mitigation activities, and to determine, in light of the estimated cost, whether it is feasible to perform the risk mitigation. In some cases, the decision may be to watch and wait, or simply to accept the risk.

Task 5:

Document initial risks and strategies in the Risk Management Plan. (PDL)

Document each initial risk, its assigned exposure, time frame, initial status, and the associated mitigation and contingency strategy, in the Risk Management Plan.

Guidance: Although the list of risks in the Risk Management Plan is not kept up-to-date, it does provide a record of the initial risk identification. The Risk Management Plan may be included in the SMP/PP.

Task 6:

Record all identified risks in the Risk Management Database. (PDL)

Record each identified risk, its assigned exposure, time frame, current status, and the associated mitigation and contingency strategy, in the approved Risk Management Database.

Guidance: The Risk Management Database is maintained and kept up-to-date for the duration of the project. New risks are included as they are identified.

Task 7:

Approve Risk Management Plan. (GSFC Project Manager and/or Branch Chief and/or Division Chief)

The appropriate levels of management should review and approve the Risk Management Plan.

Guidance: If the software effort is part of a mission-level Project, the cognizant Project Manager and responsible line manager will approve the Risk Management Plan.

Task 8:

Report risks to Project management, or enter agreed-to risks into a Project-level risk tool. (PDL, reporting to Project Manager, and possibly to Branch Head and Division Chief)

If the software effort is part of a mission-level Project, the Product Development Lead should negotiate with the cognizant Project Manager to determine precisely who will track each risk.

Guidance: The GSFC Project Manager needs to be aware of the software risks that could impact the Project. Responsibility for tracking each risk must be negotiated and clearly defined. It goes without saying that the Project will track the highest-level risks. For example, the risk that a required test bed will not be ready on time is a high-level risk and should be tracked by the Project. The responsibility for tracking lower-level risks, however, must be clearly assigned.

Measures

(See the Risk Monitoring and Control Sub-process)

Tools and Templates

Name	Description
Risk Plan Template	Standard GSFC template for preparing Risk Management Plan
FSW Risk Management Database	This database may be adapted for other branches
Risk Management Tool	Branch- or Project-selected Risk Management Tool

Check the Process Asset Library at http://software.gsfc.nasa.gov/process.cfm to obtain the latest version.
NOTE: Words or phrases shown in blue underlined contain links to additional information.
Guidance & tailoring information is shown in *italics with gray background*.

Training

Course Name	Description
NASA Continuous Risk Management Training	Identifying project risks and planning risk mitigation strategies
Risk Management Tool Training	Use of Branch- or Project-approved Risk Management Tool

References

This process is consistent with the following policies, standards, and other references.

- **NPR 8000.4:** *Risk Management Procedural Requirements*
- **NASA-STD-8739.3 (draft):** *Standard for Software Assurance*
- **GPG 7120.4:** *Risk Management*
- **GPG 8700.5:** *In-House Development and Maintenance of Software Projects*
- **580-PG-8730.3.1:** *Product Development Handbook*
- **580-PL-002-01:** *ISD Software Policies*
- **IEEE Std 1540-2001: Standard for Software Life Cycle Processes – Risk Management** (available through: http://standards.nasa.gov/npts/login.taf at http://standards.ieee.org/catalog/olis/se.html)
- **Glossary:** http://software.gsfc.nasa.gov/glossary.cfm
  Defines common terms used in ISD processes
- ***ETVX Diagram*:** Link to the ETVX diagram for this process.
- **Process Asset Library:** http://software.gsfc.nasa.gov/process.cfm
  Library of all ISD process descriptions

Quality Management System Records

Controlled Document / Description	Record Custodian
Software Risk Management Plan: Approved either by itself or as part of the SMP/PP	PDL

Development History

Version	Date	Description of Development Changes
0.1	9/10/03	Initial draft
0.2	12/29/03	Additional tasks and entry/exit criteria included
0.3	3/3/04	Risk identification and risk monitoring broken out as separate sub-processes.
0.4	3/11/04	ETVX expanded to a full process description.
0.5	4/20/04	Incorporate review comments from Linda
0.6	5/13/04	Break out ETVX into a separate file.
0.7	6/22/04	Align with June 21 version of ETVX
0.8	7/2/04	Incorporate team review comments
0.9	8/04/04	Incorporate team review comments
0.10	9/2/04	Incorporated CCB review comments

0.11	9/7/04	Incorporated CCB review comments
0.12	9/20/04	Incorporated post-CCB review comments

Change History

Version	Date	Description of Improvements
1.0	9/9/04	Approved by the ISD CCB

Check the Process Asset Library at http://software.gsfc.nasa.gov/process.cfm to obtain the latest version.
NOTE: Words or phrases shown in blue underlined contain links to additional information.
Guidance & tailoring information is shown in *italics with gray background*.

ISD Software Risk Identification

Number: 580-ED-013-01
Effective Date: September 1, 2004
Expiration Date: September 1, 2009

Approved By: (signature)
Name: Joe Hennessy
Title: Chief, ISD

Responsible Office: 580/Information Systems Division (ISD)
Title: Software Risk Identification

Asset Type: ETVX Diagram
PAL Number: 1.2.3.1

Software Risk Identification Sub-process

Inputs	Entry criteria	Major Tasks	Exit criteria	Outputs
Generic risks, if available **AND** Budget and Schedule **AND** Project-level requirements from System Concept Review or System Requirements Review **AND** Software system concept and architecture definition **AND (for reentry)** Project Monitoring and Control risk information	[All inputs are available **AND** Project Planning has begun] **OR** [Project Monitoring and Control has begun **AND** There are new risks to be identified **AND** Inputs are available	1. Identify risks 2. Estimate impact and likelihood of occurrence for each risk; combine these to estimate risk exposure 3. Classify risks 4. Develop the steps of a mitigation and/or contingency strategy for each high-exposure risk 5. Document initial risks and strategies in the Risk Management Plan 6. Record all identified risks in the Risk Management Database 7. Approve Risk Management Plan. (Guidance: This may be approved as part of the SMP/PP.) 8. Report risks to Project management, or enter them into a Project-level risk tool. **Verification & Validation** Review and approval of the Risk Management Plan	Identified risks, with mitigation and/or contingency strategies, entered in approved Risk Management Plan and Database **AND** Risks reported to Project Management (if part of a Project) **AND** Appropriate approved risks submitted for addition to generic risk set	Risk Management Plan (may be included in Product Plan) **AND** Risk Management Database **AND** Approved risks for addition to generic risk set

Check the Process Asset Library at http://software.gsfc.nasa.gov/process.cfm to obtain the latest version.
NOTE: Words or phrases shown in blue underlined contain links to additional information.
Guidance & tailoring information is shown in *italics with gray background*.

Development History

Version	Date	Change
0.1	9/10/03	Initial draft (D. Schultz)
0.2	12/29/03	Additional risk management text included: tasks and entry/exit criteria
0.3	2/10/04	Risk Management divided into two sub-processes.
0.4	5/13/04	ETVX separated from process description
0.5	6/21/04	Incorporated review comments from June 22 team meeting
0.6	7/2/04	Incorporated review comments from June 29 team meeting
0.7	7/9/04	Incorporated review comments from July 6 team meeting
0.8	7/19/04	Incorporated review comments from July 16 team meeting
0.9	8/4/04	Incorporated review comments from July 20 team meeting
0.10	9/2/04	Incorporated CCB review comments

Change History

Version	Date	Change
1.0	9/9/04	Approved by the ISD CCB

Check the Process Asset Library at http://software.gsfc.nasa.gov/process.cfm to obtain the latest version.
NOTE: Words or phrases shown in blue underlined contain links to additional information.
Guidance & tailoring information is shown in *italics with gray background*.