ISO/IEC JTC1/SC7
Software Engineering
Secretariat: CANADA (SCC)

ISO/IEC JTC1/SC7 N2461

2001-04-05

Doc. Type	Business Plan
Title	JTC1/SC7/WG9 Proposed Business Plan
Source	JTC1/SC7/WG9 Interim Convener
Project	
Status	For discussion at the upcoming plenary.
References	
Action ID	FYI or ACT
Due Date	
Mailing Date	2001-04-05
Distribution	SC7_AG; JTC1 Sec.; P, O & L Members
Medium	Encoded Acrobat
No. of Pages	5
Note	For discussion at the upcoming plenary.

Address reply to: ISO/IEC JTC1/SC7 Secretariat
Bell Canada - Quality Engineering & Research
1050 Beaver Hall Hill, 2nd Floor, Montréal (Québec) Canada H2Z 1S4
Tel.: +1 (514) 391-8286 Fax: +1 (514) 870-2246
sc7@qc.bell.ca

ISO/IEC JTC1/SC7: INFORMATION TECHNOLOGY-SOFTWARE ENGINEERING
Working Group 9: Systems and Software Integrity

Foreword

The Business Plan is maintained and updated by the Working Group Convener.

Document History

Initiated by JTC1/SC7/WG9 in Madrid 2000-05-30.

Business Plan of JTC1/SC7/WG9

1 Scope and Purpose

This Business Plan establishes the business context for ISO/IEC JTC1/SC7 WG9. The purpose of this Business Plan is to define the scope of work of the WG, its plan for meeting its business objectives, and its relationship to other SC7 WGs and to those external standardization bodies with integrity interests.

2 Customers

The customers for WG9's work products include:

- acquirers of software or systems
- suppliers of software or systems
- software or system certifiers/assessors
- regulators
- system and software standards developers
- software or system educators/trainers
- system designers/integrators (system containing software)
- software or system operators
- quality assurance and reliability practitioners
- information security personnel
- risk management and safety analysis personnel

3 Vision

A consistent, risk-based approach to defining system and software engineering practices that harmonizes existing International Standards, focuses on the interdependence of systems and software, and provides sufficient assurance that the necessary integrity characteristics of systems and software have been achieved.

4 Terms of Reference

4.1 JTC1/SC7:

Standardization of processes, supporting tools and supporting technologies for the engineering of software products and systems.

4.2 JTC1/SC7/WG9:

Standardization of processes, supporting tools and supporting technologies that assure the integrity and manage the risk associated with software products and systems, throughout the system life cycle.

5 Objectives

The business objectives of WG9 are to define a set of Integrity and Risk standards that will meet customer needs. These standards will be established through collaborative effort within the WG and harmonized with the work products of other SC7 WGs and with those external standards bodies having integrity interests.

The following summarizes the business objectives of the WG:

5.1 Harmonize the means whereby risk is taken into account in systems containing software, across specific sectors; such as aviation, medical devices, financial systems, nuclear power, communications and transportation.

5.2 Define the processes, supporting tools, and supporting technology for determining the required integrity of systems containing software.

5.3 Define the processes, supporting tools, and supporting technology for determining and managing risk associated with systems containing software.

5.4 Define the requirements on the system and software engineering practices for each integrity level that must be met in order to assure achievement of the relevant system and software quality characteristics.

5.5 Harmonize the relevant international software standards that define requirements which may vary between integrity levels.

5.6 Focus on developing standards that meet user requirements associated with integrity and risk issues.

6 Requirements for the System and Software Integrity Standards Program

6.1 Standards developed under this program shall:

6.1.1 be consistent with ISO/IEC12207 Information Technology: Software Lifecycle Processes and ISO/IEC 15288 Information Technology: Systems Lifecycle Processes.

6.1.2 be consistent with the ISO 9000 series.

6.1.3 be consistent with the IEC 300 series.

6.1.4 address how integrity and risk-related requirements are mapped into the product life cycle.

6.1.5 define the relevant management and engineering activities to ensure achievement of the required integrity.

6.1.6 define the requirements on the system and software life cycle that must be met in order for the software to meet its integrity objectives.

6.1.7 define integrity life cycle activities and results (e.g. integrity requirements, design criteria, assessment criteria, risk management criteria) at points in the product life cycle that best contribute to product value.

6.1.8 address integrity assessment as a documented life cycle process.

6.1.9 address risk management as a documented life cycle process.

6.1.10 define the ground rules and resulting documentation for integrity objectives negotiations.

6.1.11 describe the criteria for product design with specified integrity objectives.

6.1.12 define the process requirements for the integrity and risk management aspects of the software and system architecture.

6.1.13 define use of the results of integrity assessments to adjust software and systems life cycle activities in order to achieve integrity objectives.

6.1.14 address rigor of integrity and product life cycle processes and resulting information in order to be consistent with the product value and risks.

6.1.15 address integration of integrity life cycle activities with the product life cycle activities as far as is appropriate, in order to avoid unnecessary duplication of activities and documentation.

6.1.16 define the ground rules for selection and use of techniques (e.g. fault insertion, FMEA, path analysis) for determining system response to fault conditions.

6.1.17 address the selection and application of tools and techniques to be consistent with the degree of rigor determined by negotiated integrity objectives.

6.1.18 address a tailoring process for integrity life cycle activities that includes feedback from real world experiences.

6.1.19 include only system or software engineering practices which have been be verified by at least two sources from refereed journals, to a level of confidence acceptable to the majority of the active working group members.

6.1.20 describe in the document, whenever a system or software engineering practice is suggested or required in a standard or application guide, the effort associated with, and the benefits of, using or not using that practice.

6.1.21 document, in a Document Development History Folder, design decisions and supporting information regarding practices, techniques, and tools incorporated into standards and application guides. The document development history folder shall be maintained by the project editor during the course of document development and shall be archived by the working group chair at the completion of development.

6.2 The Business Plan shall be approved by letter ballot of the working group members.

7 Document Framework

7.1 Purpose

The purpose of the document framework is to describe a structure for a set of relevant standards to address users needs when dealing with integrity and risk issues related to systems and products containing software. The framework provides a rational means of identifying the requirements for pertinent standards to meet the needs of JTC1/SC7 pertaining to the scope and terms of references defined herein.

7.2 Integrity and Risk Relationship

The relationship of Integrity and Risk is established in ISO/IEC 15026: System and software integrity levels. Integrity is a system property which contains risk with acceptable limits. The integrity level is presented as a unifying concept to provide a methodology for addressing risk at the system level.

Integrity and risk are linked by the system and software operational requirements and the project objectives to minimize risk in development and performance, by minimizing risk exposure at the appropriate system and software product levels throughout the system life cycle. Software integrity and software risk management are closely related to the software life cycle processes described in the ISO/IEC 12207 standard and the ISO/IEC 9126 Software quality characteristics.

7.3 Categorization of Documents

The SC7 Functional Framework can be effectively used to categorize the set of potential integrity and risk standards for possible development within SC7/WG9. A notional document structure with example Proposed New Work Items (PNWIs) is presented in the following diagram. Relevant SC7 standards developed by WG9 and other WGs are also shown in the diagram for reference.

The document framework for Integrity and Risk Management standards is shown below:

Note: Proposed New Work Items (PNWIs) identified in this table are notional. Actual PNWIs will be specified in the WG9 Product Plan. Work items may also include SC7/WG9-TC56/WG4 Joint Working Group projects that should be transferred to SC7/WG9.

General	TR 12182

	Process	**Product**	**Tools**	**Technologies**	**Resources**	**Data**
Principle Standards	15288, 12207	9126-01, PNWI-Integrity Concepts and Applications				
Element Standards	15288, 12207, PNWI-Software Risk Management	15026, PNWI-Integrity Requirements				
Guides & Supplements	PNWI-Guidelines for Integrity Design and Assurance Process/Activity Applications	PNWI-Guidelines for Designing Integrity into Products/ Systems	PNWI-Integrity Assessment Methods	PNWI-Guidelines for Selection and Use of Technologies to Achieve Integrity Objectives	PNWI-Guidelines for Integrity Cost and Resource Requirements Estimation	PNWI-Guidelines for Analysis and Interpretation of Integrity Data

PNWI-Proposed New Work Item
TR 12182, 15026: SC7/WG9 developed standards
15288, 12207, 9126-1: Other SC7/WGs developed standards

Principle Standards: define generic principles that apply to all lower level standards. e.g. ISO/IEC 12207, Software Life Cycle Processes.

Element Standards: define requirements which apply to a defined program element. Specific requirements are grouped to facilitate tailoring of development, acquisition, and maintenance programs. e.g. ISO/IEC 15026: System and Software Integrity Levels

Guidelines: provide guidance for selection and application of relevant tools, methods and techniques.

Guide and Supplements: describe the characteristics of applying accumulated technical or management skills and methods in the creation of a product or performing a service.

8. Planning for System and Software Integrity Standards

The business needs for standardization of Software and Systems Integrity are reflected in the generic system engineering management model, and closely associated with the system and software life cycle processes for designing/building/acquiring/supporting software products and systems.

Planning for new and revised Software and Systems Integrity and Risk Management standards shall address these business needs. These needs include:

- The need to determine risk exposure and related containment
- The need to manage risk throughout the life cycle
- The need to establish integrity requirements and integrity assurance criteria
- The need to define integrity design and assurance processes/activities
- The need to validate integrity assessment methods for assurance
- The need to analyze and interpret integrity data
- The need to justify resources and expenditures on integrity and risk management efforts