IEEE Standard for Software Reviews and Audits

IEEE Computer Society

Sponsored by the
Software & Systems Engineering Standards Committee

1028™

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

15 August 2008

IEEE Std 1028™-2008
(Revision of
IEEE Std 1028-1997)

IEEE Std 1028™-2008
(Revision of
IEEE Std 1028-1997)

IEEE Standard for Software Reviews and Audits

Sponsor

Software & Systems Engineering Standards Committee
of the
IEEE Computer Society

Approved 16 June 2008

IEEE-SA Standards Board

Abstract: Five types of software reviews and audits, together with procedures required for the execution of each type, are defined in this standard. This standard is concerned only with the reviews and audits; procedures for determining the necessity of a review or audit are not defined, and the disposition of the results of the review or audit is not specified. Types included are management reviews, technical reviews, inspections, walk-throughs, and audits.
Keywords: audit, inspection, review, walk-through

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-0-7381-5768-9 STD95806
Print: ISBN 978-0-7381-5769-6 STDPD95806

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Introduction

This introduction is not part of IEEE Std 1028-2008, IEEE Standard for Software Reviews and Audits.

This introduction provides the user with the rationale and background of the reviews and audits outlined in this standard and their relationships to other IEEE standards.

Purpose

This standard defines five types of software reviews and audits, together with procedures required for the execution of each type. This standard is concerned only with the reviews and audits; it does not define procedures for determining the necessity of a review or audit, nor does it specify the disposition of the results of the review or audit. Review types include management reviews, technical reviews, inspections, and walk-throughs.

This standard is meant to be used either in conjunction with other IEEE software engineering standards or as a stand-alone definition of software review and audit procedures. In the latter case, local management must determine the events that precede and follow the actual software reviews and audits.

The need for reviews and audits is described in several other IEEE standards, as well as standards prepared by other standards-writing organizations. IEEE Std 1028-2008 is meant to support these other standards. In particular, reviews and audits required by the standards listed in Annex B can be executed using the procedures described herein. The use of IEEE Std 1044-1993 [B8][a] is encouraged as part of the reporting procedures for this standard.

General application intent

This standard applies throughout the scope of any selected software life-cycle model and provides a standard against which software review and audit plans can be prepared and assessed. Maximum benefit can be derived from this standard by planning for its application early in the project life cycle.

This standard for software reviews and audits was written in consideration of both the software and its system operating environment. It can be used where software is the total system entity or where it is part of a larger system. Care should be taken to integrate software review and audit activities into any total system life-cycle planning; software reviews and audits should exist in concert with hardware and computer system reviews and audits to the benefit of the entire system.

Reviews and audits carried out in conformance with this standard may include both personnel internal to the project and customers or acquirers of the product, according to local procedures. Suppliers may also be included if appropriate.

The information obtained during software reviews (particularly inspections) may be of benefit for improving the user's software acquisition, supply, development, operation, and maintenance processes. The use of review data for process improvement is required for inspections.

History

Major changes were made to the structure and content of IEEE Std 1028 during the last complete revision in 1997. This version was reaffirmed in 2001. As part of the reaffirmation, many balloters submitted comments. The reaffirmation was approved by the IEEE Standards Board with the proviso that the reaffirmation comments be addressed during the next revision.

[a] The numbers in brackets correspond to those of the bibliography in Annex B.

That was the context for the current revision: consider all the comments from the reaffirmation vote. Structural changes were not to be part of this effort. The Working Group considered all comments from the reaffirmation, whether accompanying negative or affirmative votes, as well as additional clarification concerns that arose during the revision.

With one exception, no structural change occurred. That exception was intended to clarify the difference between inspections and walk-throughs by requiring process improvement to be mandatory for inspections (see 6.9), and to eliminate process improvement from walk-throughs. As a result, there is a clear progression in formality from the most formal, audits, followed by management and technical reviews, then to the less formal inspections, and finishing with the least formal, walk-throughs.

Development procedure

This standard was developed by the Software Engineering Review Working Group. The entire standards writing procedure was carried out via electronic mail.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association Web site at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA Web site at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the Software Reviews Working Group had the following membership:

J. Dennis Lawrence, *Chair*

Edward Addy
T. Scott Ankrun
Chris Bagge
William Bartholomew
David Bowen
Massimo Cardaci
Norbert Carte
Michael Chonoles
Terry Dietz
Antonio Doria
Edward Dudash
Andrew Fieldsend
Gregg Giesler
Pirooz Joodi
George Kyle
David J. Leciston
Carol A. Long
Michael McCaffrey
Miroslav Pavlovic
Jamey Sanders
Helmut H. Sandmayr
Robert Schaaf
Hans Schaefer
Luca Spotorno
Thomas Starai
K. S. Subrahmanyam
Douglas Thiele
John Thuywissen

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Butch Anton
Chris Bagge
Pieter Botman
Daniel Brosnan
Juan Carreon
Norbert Carte
Lawrence Catchpole
Danila Chernetsov
Keith Chow
Raul Colcher
Paul Croll
Geoffrey Darnton
Teresa Doran
Antonio Doria
Scott P. Duncan
Kenneth D. Echeberry
Kameshwar Eranki
Carla Ewart
Harriet Feldman
Andrew Fieldsend
Andre Fournier
David Friscia
John Geldman
Gregg Giesler
Lewis Gray
Michael Grimley
John Harauz
M. Hashmi
Rutger A. Heunks
Richard Hilliard
Werner Hoelzl
Robert Holibaugh
Peter Hung
Mark Jaeger
St. Clair James
Michael C. Jett
James Jones
Piotr Karocki
Mark Knight
Thomas Kurihara
George Kyle
Marc Lacroix
Claude Y. Laporte
J. Dennis Lawrence
David J. Leciston
Yury Makedonov
Edward McCall
James Moore
Ronald G. Murias
Rajesh Murthy
Michael S. Newman
Mark Paulk
Miroslav Pavlovic
William Petit
Ulrich Pohl
Annette Reilly
Michael Roberts
Robert Robinson
Terence Rout
Randall Safier
Jamey Sanders
Helmut H. Sandmayr
Robert Schaaf
Hans Schaefer
David J. Schultz
Jungwoo Seo
Carl Singer
Luca Spotorno
Thomas Starai
Walter Struppler
Marcy Stutzman
K. S. Subrahmanyam
Douglas Thiele
John Thywissen
Thomas Tullia
Vincent J. Tume
Charlene Walrad
P. Wolfgang
Oren Yuen
Janusz Zalewski

The final conditions for approval of this standard were met on 16 June 2008. This standard was conditionally approved by the IEEE-SA Standards Board on 12 June 2008, with the following membership:

Robert M. Grow, *Chair*
Thomas Prevost, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

Victor Berman
Richard DeBlasio
Andy Drozd
Mark Epstein
Alexander Gelman
William Goldbach
Arnie Greenspan
Ken Hanus
Jim Hughes
Richard Hulett
Young Kyun Kim
Joseph L. Koepfinger*
John Kulick
David J. Law
Glenn Parsons
Ron Petersen
Chuck Powers
Narayanan Ramachandran
Jon Walter Rosdahl
Anne-Marie Sahazizian
Malcolm Thaden
Howard Wolfman
Don Wright

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Michael H. Kelley, *NIST Representative*

Lisa Perry
IEEE Standards Project Editor

Malia Zaman
IEEE Standards Program Manager, Technical Program Development

Contents

1. Overview 1

1.1 Scope 1
1.2 Purpose 2
1.3 Relationship with IEEE Std 12207-2008 2
1.4 Conformance 2
1.5 Organization of this standard 3
1.6 Application of this standard 3

2. Normative references 5

3. Definitions 5

4. Management reviews 6

4.1 Introduction to management reviews 6
4.2 Responsibilities 7
4.3 Input 9
4.4 Entry criteria 9
4.5 Procedures 9
4.6 Exit criteria 11
4.7 Output 11

5. Technical reviews 11

5.1 Introduction to technical reviews 11
5.2 Responsibilities 12
5.3 Input 13
5.4 Entry criteria 13
5.5 Procedures 14
5.6 Exit criteria 16
5.7 Output 16

6. Inspections 16

6.1 Introduction to inspections 16
6.2 Responsibilities 17
6.3 Input 18
6.4 Entry criteria 19
6.5 Procedures 20
6.6 Exit criteria 23
6.7 Output 23
6.8 Data collection 23
6.9 Improvement 25

7. Walk-throughs 25

7.1 Introduction to walk-throughs 25
7.2 Responsibilities 26
7.3 Input 26

7.4 Entry criteria 27
7.5 Procedures 27
7.6 Exit criteria 29
7.7 Output 29
7.8 Data collection recommendations 29
7.9 Improvement 30

8. Audits 30

8.1 Introduction to audits 30
8.2 Responsibilities 31
8.3 Input 33
8.4 Entry criteria 33
8.5 Procedures 34
8.6 Exit criteria 36
8.7 Output 37

Annex A (informative) Comparison of review types 38

Annex B (informative) Bibliography 40

IEEE Standard for Software Reviews and Audits

IMPORTANT NOTICE: This standard is not intended to assure safety, security, health, or environmental protection in all circumstances. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

1. Overview

1.1 Scope

This standard provides minimum acceptable requirements for systematic software reviews, where "systematic" includes the following attributes:

- Team participation
- Documented results of the review
- Documented procedures for conducting the review

Reviews that do not meet the requirements of this standard are considered to be non-systematic reviews. The standard is not intended to discourage or prohibit the use of non-systematic reviews.

The definitions, requirements, and procedures for the following five types of reviews are included within this standard:

a) Management reviews
b) Technical reviews
c) Inspections
d) Walk-throughs
e) Audits

This standard does not establish the need to conduct specific reviews; that need is defined by other software engineering standards or by local procedures. This standard provides definitions, requirements, and procedures that are applicable to the reviews of software development products throughout the software life cycle. Users of this standard shall specify where and when this standard applies and any intended deviations from this standard.

This standard may be used with other software engineering standards that determine the products to be reviewed, the timing of reviews, and the necessity of reviews. This standard is closely aligned with IEEE Std 1012™-2004 [B6], but it can also be used with IEEE Std 1074™-2006 [B11], IEEE Std 730™-2002 [B2], IEEE Std 12207™-2008 [B15], and other standards.[1] A useful model is to consider IEEE Std 1028-2008 as a subroutine to the other standards. Thus, if IEEE Std 1012-2004 [B6] were used to carry out the verification and validation process, the procedure in IEEE Std 1012-2004 [B6] could be followed until such time as instructions to carry out a specific review are encountered. At that point, IEEE Std 1028-2008 would be "called" to carry out the review, using the specific review type described herein. Once the review has been completed, IEEE Std 1012-2004 [B6] would be "returned to" for disposition of the results of the review and any additional action required by IEEE Std 1012-2004 [B6].

This standard may also be used as a stand-alone definition of software review and audit procedures. In this case, local management must determine the events that precede and follow the actual software reviews and audits.

In this model, requirements and quality attributes for the software product are "parameter inputs" to the review and are imposed by the "caller." When the review is finished, the review outputs are "returned" to the "caller" for action. Review outputs typically include anomaly lists and action item lists; the resolution of the anomalies and action items are the responsibility of the "caller."

1.2 Purpose

The purpose of this standard is to define systematic reviews and audits applicable to software acquisition, supply, development, operation, and maintenance. This standard describes how to carry out a review. Other standards or local management define the context within which a review is performed, and the use made of the results of the review. Software reviews can be used in support of the objectives of project management, system engineering (for example, functional allocation between hardware and software), verification and validation, configuration management, quality assurance, and auditing. Different types of reviews reflect differences in the goals of each review type. Systematic reviews are described by their defined procedures, scope, and objectives.

1.3 Relationship with IEEE Std 12207-2008

This standard may be used to achieve the outcomes of 7.2.6 (Software Review Process) and 7.2.7 (Software Audit Process) of IEEE Std 12207-2008 [B15].

1.4 Conformance

Conformance to this standard for a specific review type can be claimed when all mandatory actions (indicated by "shall") are carried out as defined in this standard for the review type used. Claims for conformance should be phrased to indicate the review types used, for example, "conforming to IEEE Std 1028-2008 for inspections." The word "shall" is used to express a requirement, "should," to express a recommendation, and "may," to express alternative or optional methods of satisfying a requirement.

[1] The numbers in brackets correspond to those of the bibliography in Annex B.

1.5 Organization of this standard

Clause 4 to Clause 8 of this standard provide guidance and descriptions for the five types of systematic reviews addressed by this standard. Each of these clauses contains the following information:

a) *Introduction to review.* Describes the objectives of the systematic review and provides an overview of the systematic review procedures.

b) *Responsibilities.* Defines the roles and responsibilities needed for the systematic review.

c) *Input.* Describes the requirements for input needed by the systematic review.

d) *Entry criteria.* Describes the criteria to be met before the systematic review can begin, including the following:

   1) Authorization

   2) Initiating event

e) *Procedures.* Details the procedures for the systematic review, including the following:

   1) Planning the review

   2) Overview of procedures

   3) Preparation

   4) Examination/evaluation/recording of results

   5) Rework/follow-up

f) *Exit criteria.* Describes the criteria to be met before the systematic review can be considered complete.

g) *Output.* Describes the minimum set of deliverables to be produced by the systematic review.

1.6 Application of this standard

The procedures and terminology defined in this standard apply to software acquisition, supply, development, operation, and maintenance processes requiring systematic reviews. Systematic reviews are performed on a software product as required by other standards or local procedures.

The term “software product” is used in this standard in a very broad sense. Examples of software products include, but are not limited to, the following:

— Anomaly reports

— Audit reports

— Backup and recovery plans

— Build procedures

— Contingency plans

— Contracts

— Customer or user representative complaints

— Disaster plans

— Hardware performance plans

— Inspection reports

- Installation plans
- Installation procedures
- Maintenance manuals
- Maintenance plans
- Management review reports
- Operations and user manuals
- Procurement and contracting methods
- Progress reports
- Release notes
- Reports and data (for example, review, audit, project status, anomaly reports, test data)
- Request for proposal
- Risk management plans
- Software quality assurance plans (see IEEE Std 730™-2002 [B2])
- Software configuration management plans (see IEEE Std 828™-2005 [B3])
- Software test documentation (see IEEE Std 829™-2008 [B4])
- Software requirements specifications (see IEEE Std 830™-1998 [B5])
- Software verification and validation plans (see IEEE Std 1012™-2004 [B6])
- Software design descriptions (see IEEE Std 1016™-1998 [B7])
- Software project management plans (see IEEE Std 1058™-1998 [B9])
- Software user documentation (see IEEE Std 1063™-2001 [B10])
- Software safety plans (see IEEE Std 1228™-1994 [B13])
- Software architectural descriptions (see IEEE Std 1471™-2000 [B14])
- Source code
- Specifications
- Standards, regulations, guidelines, and procedures
- System build procedures
- Technical review reports
- Vendor documents
- Walk-through reports

This standard permits reviews to be held by means other than physically meeting in a single location. Examples include telephone conferences, video conferences, Internet Web conferences and other means of group electronic communication. In such cases, the communication means should be defined in addition to the meeting places, and all other review requirements remain applicable.

In order to make use of this standard to carry out a software review, first decide the objective of the review. Next, select an appropriate review type. Then follow the procedure described in the appropriate clause (Clause 4 through Clause 8) of this standard.

If unforeseen events or problems cause any review to fail or terminate, the review process should report this result to the invoking process. This reporting process should be consistent with other process problem reporting standards used by the organization, which are not within the scope of this review process standard.

2. Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated referenced, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 610.12™-1990, IEEE Standard Glossary of Software Engineering Terminology.[2, 3]

NOTE—Additional standards that may be used to prepare software products that are the subject of reviews or audits are cited in the bibliography in Annex B.[4]

3. Definitions

For purposes of this standard, the following terms and definitions apply. IEEE Std 610.12-1990 and *The Authoritative Dictionary of IEEE Standards Terms* [B1] should be consulted for terms not defined in this clause.[5]

NOTE 1—Six of the terms given here are defined in other IEEE software engineering standards. The definition of the term "anomaly" is identical to that given in IEEE Std 1044™-1993 [B8]. The terms "audit," "inspection," "review," "software product," and "walk-through" are all defined in IEEE Std 610.12-1990; however, some minor modifications have been made to those definitions to more closely match the content of this standard, as explained in the succeeding paragraphs.

NOTE 2—IEEE Std 610.12-1990 uses different terms for the object of a review: audits and reviews are defined therein in terms of "work products," inspections are defined in terms of "development products," and walk-throughs are defined in terms of "segment of documentation or code." "Work products" are not defined in IEEE Std 610.12-1990. Since "software product" is defined therein, and it is desirable to use a single term in this standard, a change in terminology was made. Since software products being reviewed are not limited to those "designated for delivery to a user," that phrase was dropped from the definition of "software product." The definition of "inspection" has been changed considerably.

3.1 anomaly: Any condition that deviates from expectations based on requirements specifications, design documents, user documents, standards, etc., or from someone's perceptions or experiences.

NOTE—Anomalies may be found during, but not limited to, the review, test, analysis, compilation, or use of software products or applicable documentation.

3.2 audit: An independent examination of a software product, software process, or set of software processes performed by a third party to assess compliance with specifications, standards, contractual agreements, or other criteria.

NOTE—An audit should result in a clear indication of whether the audit criteria have been met.

[2] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).
[3] The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.
[4] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.
[5] Information on references can be found in Clause 2.

3.3 inspection: A visual examination of a software product to detect and identify software anomalies, including errors and deviations from standards and specifications.

NOTE—Inspections are peer examinations led by impartial facilitators who are trained in inspection techniques. Determination of remedial or investigative action for an anomaly is a mandatory element of a software inspection, although the solution should not be determined in the inspection meeting.

3.4 management review: A systematic evaluation of a software product or process performed by or on behalf of management that monitors progress, determines the status of plans and schedules, confirms requirements and their system allocation, or evaluates the effectiveness of management approaches used to achieve fitness for purpose.

3.5 review: A process or meeting during which a software product, set of software products, or a software process is presented to project personnel, managers, users, customers, user representatives, auditors or other interested parties for examination, comment or approval.

3.6 software product: (A) A complete set of computer programs, procedures, and associated documentation and data. **(B)** One or more of the individual items in **(A)**.

3.7 technical review: A systematic evaluation of a software product by a team of qualified personnel that examines the suitability of the software product for its intended use and identifies discrepancies from specifications and standards.

NOTE—Technical reviews may also provide recommendations of alternatives and examination of various alternatives.

3.8 walk-through: A static analysis technique in which a designer or programmer leads members of the development team and other interested parties through a software product, and the participants ask questions and make comments about possible anomalies, violation of development standards, and other problems.

4. Management reviews

4.1 Introduction to management reviews

The purpose of a management review is to monitor progress, determine the status of plans and schedules, or evaluate the effectiveness of management approaches used to achieve fitness for purpose. Management reviews support decisions about corrective actions, changes in the allocation of resources, or changes to the scope of the project.

Management reviews identify consistency with and deviations from plans, or adequacies and inadequacies of management procedures. Technical knowledge may be necessary to conduct a successful management review. The examination may require more than one meeting. The examination need not address all aspects of the software product or process.

Examples of software products subject to management review include, but are not limited to, the following:

- Anomaly reports
- Audit reports
- Backup and recovery plans
- Contingency plans
- Specifications

- Customer or user representative complaints
- Disaster plans
- Hardware performance plans
- Installation plans
- Maintenance plans
- Procurement and contracting methods
- Progress reports
- Risk management plans
- Software configuration management plans
- Software project management plans
- Software quality assurance plans
- Software safety plans
- Software verification and validation plans
- Technical review reports
- Software product analyses
- Verification and validation reports
- Migration strategy and plans
- Test results
- Software development process descriptions
- Software architectural descriptions

Examples of software processes (see IEEE Std 12207-2008 [B15]) subject to management review include, but are not limited to, the following:

- Acquisition and supply processes
- Development, operation, and maintenance processes
- Documentation process
- Configuration management process
- Quality assurance process
- Verification, validation, joint review, and audit processes
- Problem resolution processes
- Management, improvement, and infrastructure process
- Training process

4.2 Responsibilities

Management reviews are carried out by, or on behalf of, the management personnel having responsibility for the system. Management reviews shall be performed by the available personnel who are best qualified to evaluate the software product or process.

The following roles shall be established for the management review:

a) Decision maker

b) Review leader

c) Recorder

d) Management staff

e) Technical staff

The following roles may also be established for the management review:

f) Other team members

g) Customer representative

h) User representative

A person may occupy more than one role but never all of them. A role may be served by more than one individual.

4.2.1 Decision maker

The decision maker is the person for whom the management review is conducted. The decision maker shall determine if the review objectives have been met.

4.2.2 Review leader

The review leader shall ensure that administrative tasks pertaining to the review are completed, shall be responsible for planning and preparation as described in 4.5.2 and 4.5.4, shall ensure that the review is conducted in an orderly manner and meets its objectives, and shall issue the review outputs as described in 4.7.

4.2.3 Recorder

The recorder shall document anomalies, action items, decisions, and recommendations made by the review team.

4.2.4 Management staff

Management staff assigned to carry out management reviews shall actively participate in the review. Managers responsible for the system as a whole may have additional responsibilities as defined in 4.5.1.

4.2.5 Technical staff

The technical staff shall provide the information necessary for the management staff to fulfill its responsibilities.

4.2.6 Customer or user representative

The role of the customer or user representative should be determined by the review leader prior to the review.

4.3 Input

Input to the management review shall include the following:

a) A statement of objectives for the management review

b) The software product or process being evaluated

c) Software project management plan

d) Status, relative to plan, of the software product or process completed or in progress

e) Current anomalies or issues list

f) Documented review procedures

g) List of actions from previous review on the same software product or process, if such exists

Input to the management review should also include the following:

h) Status of resources, including finance, as appropriate

i) Anomaly categories (see IEEE Std 1044-1993 [B8])

j) Risk assessment reports

Additional reference material may be made available by the individuals responsible for the software product or process when requested by the review leader.

4.4 Entry criteria

4.4.1 Authorization

The need for conducting management reviews should initially be established in the appropriate project planning documents, as listed in 4.1. Under these plans, completion of a specific software product, process, or process activity may initiate a management review. In addition to those management reviews required by a specific plan, other management reviews may be announced and held at the request of software quality management, functional management, project management, or the customer or user representative, according to local procedures.

4.4.2 Preconditions

A management review shall be conducted only when both of the following conditions have been met:

a) A statement of objectives for the review is established by the management personnel for whom the review is being carried out.

b) The required review inputs are available with the required notice period to enable all participants to become fully aware of them.

4.5 Procedures

4.5.1 Management preparation

Managers shall ensure that the review is performed as required by applicable standards and procedures and by requirements mandated by law, contract, or other policy. To this end, managers shall do the following:

a) Plan time and resources required for reviews, including support functions, as required in IEEE Std 1058-1998 [B9] or other appropriate standards

b) Provide funding and facilities required to plan, define, execute, and manage the reviews

c) Provide training and orientation on review procedures applicable to a given project

d) Ensure appropriate levels of expertise and knowledge sufficient to comprehend the software product or process under review

e) Ensure that planned reviews are conducted

f) Act on review team recommendations in a timely manner

4.5.2 Planning the review

The review leader shall be responsible for the following activities:

a) Identify, with appropriate management support, the review team

b) Assign specific responsibilities to the review team members

c) Schedule and announce the meeting

d) Distribute review materials to participants, allowing adequate time for their preparation

e) Set a timetable for distribution of review material, the return of comments, and forwarding of comments to the author for disposition

4.5.3 Overview of review procedures

A qualified person should present an overview session for the review team when requested by the review leader. This overview may occur as part of the review meeting (see 4.5.5) or as a separate meeting.

4.5.4 Preparation

Each review team member shall examine the software product or process and other review inputs prior to the review meeting. Anomalies detected during this examination should be documented and sent to the review leader. The review leader should ensure that anomalies are classified so that review meeting time is used most effectively. The review leader should forward the anomalies to the author of the software product or owner of the software process for disposition.

4.5.5 Examination

The management review shall consist of one or more meetings of the review team. The meetings shall accomplish the following goals:

a) Review the objectives of the management review

b) Evaluate the software product or process under review against the review objectives

c) Evaluate project status, including the status of plans and schedules

d) Review anomalies identified by the review team prior to the review

e) Generate a list of action items, emphasizing risks

f) Document the meeting

The meetings should accomplish the following goals as appropriate:

g) Evaluate and manage the risk issues that may jeopardize the success of the project

h) Resource allocation changes and project redirection and replanning

i) Confirm software requirements and their system allocation

j) Decide the course of action to be taken or recommendations for action

k) Identify other issues that should be addressed

4.5.6 Rework/follow-up

The review leader shall verify that the action items assigned in the meeting are closed.

4.6 Exit criteria

The management review shall be considered complete when the activities listed in 4.5.5 have been accomplished and the output described in 4.7 exists.

4.7 Output

The output from the management review shall be documented evidence that identifies the following:

a) The product or process being reviewed

b) The review team members

c) Review objectives

d) Specific inputs to the review

e) Action item status (open, closed), ownership and target date (if open), or completion date (if closed)

f) A list of anomalies identified by the review team that shall be addressed for the project to meet its goals

Although this standard sets minimum requirements for the content of the documented evidence, it is left to local procedures to prescribe additional content, format requirements, and media.

The review output shall be delivered to the decision maker or other responsible management as determined by local procedures. The review output shall also be delivered to the affected project personnel.

5. Technical reviews

5.1 Introduction to technical reviews

The purpose of a technical review is to evaluate a software product by a team of qualified personnel to determine its suitability for its intended use and identify discrepancies from specifications and standards. It provides management with evidence to confirm the technical status of the project.

Technical reviews may also provide the recommendation and examination of various alternatives, which may require more than one meeting. The examination need not address all aspects of the product.

Examples of software products subject to technical review include, but are not limited to, the following:

— Software requirements specification
— Software design description
— Software test documentation
— Software user documentation
— Maintenance manual
— System build procedures
— Installation procedures
— Release notes
— Specifications
— Software development process descriptions
— Software architectural descriptions

5.2 Responsibilities

The following roles shall be established for the technical review:

a) Decision maker
b) Review leader
c) Recorder
d) Technical reviewer

The following roles may also be established for the technical review:

e) Management staff
f) Other team members
g) Other stakeholders such as managers, technical staff, customers, and users

Individual participants may act in more than one role, but no individual should act in all roles.

5.2.1 Decision maker

The decision maker is the person for whom the technical review is conducted. The decision maker shall determine if the review objectives have been met.

5.2.2 Review leader

The review leader shall be responsible for the review. This responsibility includes performing administrative tasks pertaining to the review, ensuring that the review is conducted in an orderly manner, and ensuring that the review meets its objectives. The review leader shall issue the review outputs as described in 5.7.

5.2.3 Recorder

The recorder shall document anomalies, action items, decisions, and recommendations made by the review team.

5.2.4 Technical reviewer

Staff in a technical role shall actively participate in the review and evaluation of the software product.

5.2.5 Management staff

Staff in a management role may participate in the technical review for the purpose of identifying issues that require management resolution.

5.2.6 Customer or user representative

The review leader should determine the need for a customer or user representative with respect to the particular review, and define the scope of such a representative in this role during the review.

5.3 Input

Input to the technical review shall include the following:

a) A statement of objectives for the technical review

b) The software product being examined

c) Current anomalies or issues list for the software product

d) Documented review procedures

Input to the technical review should also include the following:

e) Relevant review reports

f) Any regulations, standards, guidelines, plans, specifications, and procedures against which the software product is to be examined

g) Review support material like forms, checklists, rules, and anomaly categorization (see IEEE Std 1044-1993 [B8])

Additional reference material may be made available by the individuals responsible for the software product when requested by the review leader.

5.4 Entry criteria

5.4.1 Authorization

The need for conducting technical reviews of a software product shall be defined by project documents, such as project plans, quality assurance plans, safety plans, etc. In addition to those technical reviews required by a specific plan, other technical reviews may be announced and held upon authorization by functional management, project management, software quality management, systems engineering, or software engineering according to local procedures. Technical reviews may be required to evaluate impacts of hardware or third-party product anomalies or deficiencies on the software product.

5.4.2 Preconditions

A technical review shall be conducted only when the required review inputs are available and the people assigned to roles have been adequately trained.

5.5 Procedures

5.5.1 Management preparation

Managers should ensure that the review is performed as required by applicable standards and procedures and by requirements mandated by law, contract, or other policy. To this end, managers should do the following:

a) Plan time and resources required for reviews, including support functions, as required in IEEE Std 1058-1998 [B9] or other appropriate standards

b) Provide funding and facilities required to plan, define, execute, and manage the reviews

c) Provide training and orientation on review procedures applicable to a given project

d) Ensure that reviewers are available with an appropriate level of skills, expertise, and knowledge sufficient to comprehend the software product under review.

NOTE—The review leader is responsible for selecting reviewers, and the management is responsible for making them available.

e) Ensure that planned reviews are conducted

f) Act on review team recommendations in a timely manner

5.5.2 Planning the review

The review leader shall be responsible for the following activities:

a) Identify, with appropriate management support, the review team

b) Assign specific responsibilities to the review team members

c) Schedule and announce the meeting place

d) Distribute review materials to participants, allowing adequate time for their preparation

e) Set a timetable for distribution of review material, the return of comments, and forwarding of comments to the author for disposition

As a part of the planning procedure, the review team shall determine if alternatives are to be discussed at the review meeting. Alternatives may be discussed at the review meeting, afterwards in a separate meeting, or left to the author of the software product to resolve.

5.5.3 Overview of review procedures

A qualified person should present an overview of the review procedures for the review team when requested by the review leader. This overview may occur as a part of the review meeting (see 5.5.6) or as a separate meeting.

5.5.4 Overview of the software product

A technically qualified person should present an overview of the software product for the review team when requested by the review leader. This overview may occur either as a part of the review meeting (see 5.5.6) or as a separate meeting.

5.5.5 Preparation

Each review team member shall examine the software product and other review inputs prior to the review meeting. Anomalies detected during this examination should be documented and sent to the review leader. The review leader should classify anomalies to ensure that review meeting time is used most effectively. The review leader should forward the anomalies to the author of the software product for disposition.

The review leader shall verify that the team members are prepared for the review meeting. If a reviewer has not prepared adequately, the review leader shall take corrective action, such as finding a stand-in, assigning the reviewer's tasks to other reviewers, or rescheduling the meeting.

5.5.6 Examination

During the technical review, the review team shall hold one or more meetings. The meetings shall accomplish the following goals:

a) Decide on the agenda for evaluating the software product and anomalies

b) Determine if

   1) The software product is complete

   2) The software product conforms to the regulations, standards, guidelines, plans, specifications, specifications, and procedures applicable to the project

   3) If applicable, changes to the software product are properly implemented and affect only the specified areas

   4) The software product is suitable for its intended use

   5) The software product is ready for the next activity

   6) The findings of the inspection necessitates a change in the software project schedule

   7) Anomalies exist in other system elements such as hardware or external/complementary software

c) Identify anomalies and decide their criticality

NOTE—Assignment of action items is left to management follow-up.

d) Generate a list of action items, emphasizing risks

e) Document the meeting

After the software product has been reviewed, documentation shall be generated to document the meeting, list anomalies found in the software product, and describe any recommendations to management.

When anomalies are sufficiently critical or numerous, the review leader should recommend that an additional review be applied to the modified software product. This, at a minimum, should cover product areas changed to resolve anomalies as well as side effects of those changes.

5.5.7 Rework/follow-up

The review leader shall verify that the action items assigned in the meeting are closed.

5.6 Exit criteria

A technical review shall be considered complete when the activities listed in 5.5.6 have been accomplished and the output described in 5.7 exists.

5.7 Output

The output from the technical review shall consist of documented evidence that identifies the following:

a) The project being reviewed

b) The review team members

c) The software product reviewed

d) Specific inputs to the review

e) Review objectives and whether they were met

f) A list of software product anomalies

g) A list of unresolved system or hardware anomalies or specification action items

h) A list of management issues

i) Action item status (open, closed), ownership and target date (if open), or completion date (if closed)

j) Any recommendations made by the review team on how to dispose of unresolved issues and anomalies

k) Whether the software product meets the applicable regulations, standards, guidelines, plans, specifications, and procedures without deviations

Although this standard sets minimum requirements for the content of the documented evidence, it is left to local procedures to prescribe additional content, format requirements, and media.

6. Inspections

6.1 Introduction to inspections

The purpose of an inspection is to detect and identify software product anomalies. An inspection is a systematic peer examination that does one or more of the following:

a) Verifies that the software product satisfies its specifications

b) Verifies that the software product exhibits specified quality attributes

c) Verifies that the software product conforms to applicable regulations, standards, guidelines, plans, specifications, and procedures

d) Identifies deviations from provisions of item a), item b), and c)

e) Collects software engineering data (for example, anomaly and effort data)

f) Provides the collected software engineering data that may be used to improve the inspection process itself and its supporting documentation (for example, checklists)

g) Requests or grants waivers for violation of standards where the adjudication of the type and extent of violations are assigned to the inspection jurisdiction

h) Uses the data as input to project management decisions as appropriate (e.g., to make trade-offs between additional inspections versus additional testing)

Inspections consist of two to six participants (including the author). An inspection is led by an impartial trained facilitator who is trained in inspection techniques. Determination of remedial or investigative action for an anomaly is a mandatory element of a software inspection, although the resolution should not occur in the inspection meeting. Collection of data for the purpose of analysis and improvement of software engineering procedures is a mandatory element of software inspections.

Examples of software products subject to inspections include, but are not limited to, the following:

— Software requirements specification

— Software design description

— Source code

— Software test documentation

— Software user documentation

— Maintenance manual

— System build procedures

— Installation procedures

— Release notes

— Software models

— Specifications

— Software development process descriptions

— Policies, strategies, and plans

— Marketing and publicity documents

— Software architectural descriptions

6.2 Responsibilities

The following roles shall be established for the inspection:

a) Inspection leader

b) Recorder

c) Reader

d) Author

e) Inspector

All participants in the inspection are inspectors. The author should not act as inspection leader and shall not act as reader or recorder. Other roles may be shared among the team members. Individual participants may act in more than one role.

Individuals holding management positions over any member of the inspection team shall not participate in the inspection.

6.2.1 Inspection leader

The inspection leader shall be responsible for planning and organizational tasks pertaining to the inspection, shall determine the parts/components of the software product and source documents to be inspected during the meeting (in conjunction with the author), shall be responsible for planning and preparation as described in 6.5.2 and 6.5.4, shall ensure that the inspection is conducted in an orderly manner and meets its objectives, shall ensure that the inspection data is collected, and shall issue the inspection output as described in 6.7.

6.2.2 Recorder

The recorder shall document anomalies, action items, decisions, waivers, and recommendations made by the inspection team. The recorder should record inspection data required for process analysis. The inspection leader may be the recorder.

6.2.3 Reader

The reader shall lead the inspection team through the software product in a comprehensive and logical fashion, interpreting sections of the work (for example, generally paraphrasing groups of 1 to 3 lines), and highlighting important aspects. The software product may be divided into logical sections and assigned to different readers to lessen required preparation time.

6.2.4 Author

The author shall be responsible for the software product meeting its inspection entry criteria, for contributing to the inspection based on special understanding of the software product, and for performing any rework required to make the software product meet its inspection exit criteria.

6.2.5 Inspector

Inspectors shall identify and describe anomalies in the software product. Inspectors shall be chosen based on their expertise and should be chosen to represent different viewpoints at the meeting (for example, sponsor, end user, requirements, design, code, safety, test, independent test, project management, quality management, and hardware engineering). Only those viewpoints pertinent to the inspection of the product should be present.

Some inspectors should be assigned specific topics to ensure effective coverage. For example, one inspector may focus on conformance with a specific standard or standards, another on syntax or accuracy of figures, and another for overall coherence. These viewpoints should be assigned by the inspection leader when planning the inspection, as provided in item b) of 6.5.2.

6.3 Input

Input to the inspection shall include the following:

a) A statement of objectives for the inspection

b) The software product(s) to be inspected

c) Documented inspection procedure

d) Inspection reporting forms

e) Anomalies or issues list

f) Source documents such as specifications and software product inputs that serve as documents that have been used by the author as inputs to development the software product

Input to the inspection may also include the following:

g) Inspection checklists

h) Quality criteria for requiring a reinspection

i) Predecessor software product that has previously been inspected, approved, or established as a baseline

j) Any regulations, standards, guidelines, plans, specifications, and procedures against which the software product is to be inspected

k) Hardware, instrumentation, or other software product specifications

l) Performance data

m) Anomaly categories (see IEEE Std 1044-1993 [B8])

Additional reference material may be made available by the individuals responsible for the software product when requested by the inspection leader.

6.4 Entry criteria

6.4.1 Authorization

Inspections shall be planned and documented in the appropriate project planning documents (for example, the project plan, the software quality assurance plan, or the software verification and validation plan).

Additional inspections may be conducted during acquisition, supply, development, operation, and maintenance of the software product at the request of project management, quality management, or the author, according to local procedures.

6.4.2 Preconditions

An inspection shall be conducted only when the relevant inspection inputs are available.

6.4.3 Minimum entry criteria

An inspection shall not be conducted until all of the following events have occurred, unless there is a documented rationale, accepted by management, for exception from these provisions:

a) The inspection leader determines that the software product to be inspected is complete and conforms to project standards for format.

b) Automated error-detecting tools (such as spell-checkers and compilers) have been used to identify and eliminate errors prior to the inspection.

c) Prior milestones upon which the software product depends are satisfied as identified in the appropriate planning documents.

d) Required supporting documentation is available.

e) For a reinspection, all items noted on the anomaly list that affect the software product under inspection are resolved.

6.5 Procedures

6.5.1 Management preparation

Management shall ensure that the inspection is performed as required by applicable standards and procedures and by requirements mandated by law, contract, or other policy. To this end, managers shall do the following:

a) Plan time and resources required for inspection, including support functions, as required in IEEE Std 1058-1998 [B9] or other appropriate standards

b) Provide funding, infrastructure, and facilities required to plan, define, execute, and manage the inspection

c) Provide training and orientation on inspection procedures applicable to a given project

d) Ensure that inspection team members possess appropriate levels of expertise and knowledge sufficient to comprehend the software product under inspection

e) Ensure that inspections are planned, and that planned inspections are conducted

f) Act on inspection team recommendations in a timely manner

6.5.2 Planning the inspection

The author shall assemble the inspection materials for the inspection leader. Inspection materials include the software product to be inspected, standards and documents that have been used to develop the software product, etc.

The inspection leader shall be responsible for the following activities:

a) Identify, with appropriate management support, the inspection team

NOTE—Ensure that inspection team members possess appropriate levels of expertise and knowledge sufficient to comprehend the software product to be inspected as well as the documents used by the author to develop the software product.

b) Assign specific responsibilities to the inspection team members

c) Schedule the meeting date and time, select the meeting place, and notify the inspection team

d) Distribute inspection materials to participants, and allow adequate time for their preparation

e) Set a timetable for distribution of inspection material and for the return of comments and forwarding of comments to the author for disposition

f) Specify the scope of the inspection, including the priority of sections of the documents to be inspected

The inspection leader should be responsible for the following activity:

g) Establish the anticipated inspection rate for preparation and meeting

NOTE—In many cases, the anticipated inspection rate is a critical element of inspection planning. The following table provides guidelines for typical inspection rates and anomaly recording rates, in terms of pages or lines of code per hour:

Type of document inspected	Inspection rate
Architecture	2 PPH to 3 PPH (see NOTE 1)
Requirements	2 PPH to 3 PPH
Preliminary design	3 PPH to 4 PPH
Detailed design	3 PPH to 4 PPH
Source code	100 PPH to 200 LPH (see NOTE 2)
Test plan	5 PPH to 7 PPH
Fixes and changes	50 PPH to 75 LPH
User documentation	8 PPH to 20 PPH
NOTE 1—Page per hour. NOTE 2—Lines (of code) per hour.	

6.5.3 Overview of inspection procedures

Roles shall be assigned by the inspection leader. The inspection leader shall answer questions about any checklists and the role assignments and should present inspection data such as minimal preparation times, the recommended inspection rate, and the typical number of anomalies previously found in inspections of similar products.

6.5.4 Overview of inspection product

The author should present an overview of the software product to be inspected. This overview should be used to introduce the inspectors to the software product. The overview may be attended by other project personnel who could profit from the presentation.

6.5.5 Preparation

Each inspection team member shall examine the software product and other inputs prior to the review meeting. Anomalies detected during this examination shall be documented and sent to the inspection leader. The inspection leader should classify anomalies as described in 6.8.1 to determine whether they warrant cancellation of the inspection meeting, and in order to plan efficient use of time in the inspection meeting. If the inspection leader determines that the extent or seriousness of the anomalies warrants, the inspection leader may cancel the inspection, requesting a later inspection when the software product meets the minimal entry criteria and is reasonably defect-free. The inspection leader should forward the anomalies to the author of the software product for disposition.

The inspection leader or reader shall specify a suitable order in which the software product will be inspected (such as sequential, hierarchical, data flow, control flow, bottom up, or top down). The reader(s) shall prepare sufficiently to be able to present the software product at the inspection meeting.

The inspection leader shall verify that inspectors are prepared for the inspection. The inspection leader shall reschedule the meeting if the inspectors are not adequately prepared. The inspection leader should gather individual preparation times and record the total in the inspection documentation.

6.5.6 Examination

The inspection meeting shall follow the agenda as described in 6.5.6.1 through 6.5.6.5.

6.5.6.1 Introduce meeting

The inspection leader shall introduce the participants and describe their roles. The inspection leader shall state the purpose of the inspection and should remind the inspectors to focus their efforts toward anomaly detection, not resolution. The inspection leader shall remind the inspectors to direct their remarks to the recorder and to comment only on the software product, not its author. Inspectors may pose questions to the author regarding the software product. The inspection leader shall resolve any special procedural questions raised by the inspectors. Extensive discussion about issues should be postponed to the end of the meeting or to a separate meeting.

6.5.6.2 Review general items

Anomalies referring to the software product in general (and thus not attributable to a specific instance or location) shall be presented to the inspectors and recorded.

6.5.6.3 Review software product and record anomalies

The reader shall present the software product to the inspection team. The inspection team shall examine the software product objectively and thoroughly, and the inspection leader shall focus this part of the meeting on creating the anomaly list. The recorder shall enter each anomaly, location, description, and classification on the anomaly list. IEEE Std 1044-1993 [B8] may be used to classify anomalies. During this time, the author shall answer specific questions and contribute to anomaly detection based on the author's understanding of the software product. If there is disagreement about an anomaly, the potential anomaly shall be logged and marked for resolution at the end of the meeting.

6.5.6.4 Review the anomaly list

At the end of the inspection meeting, the inspection leader shall have the anomaly list reviewed with the team to ensure its completeness and accuracy. The inspection leader shall allow time to discuss every anomaly when disagreement occurred. The inspection leader shall not allow the discussion to focus on resolving the anomaly but on clarifying what constitutes the anomaly. If a disagreement as to the existence or severity of an anomaly cannot be quickly resolved during the meeting, that disagreement shall be documented in the anomaly report.

6.5.6.5 Make exit decision

The purpose of the exit decision is to bring an unambiguous closure to the inspection meeting. The exit decision shall determine if the software product meets the inspection exit and quality criteria. As part of this decision, any appropriate rework and verification shall be prescribed. Specifically, the inspection team shall identify the software product disposition as one of the following:

a) *Accept with no verification or with rework verification.* The software product is accepted as is or with only minor rework (for example, that would require no further verification).

b) *Accept with rework verification.* The software product is to be accepted after the inspection leader or a designated member of the inspection team (other than the author) verifies rework.

c) *Reinspect.* The software product cannot be accepted. Once anomalies have been resolved a reinspection should be scheduled to verify rework. At a minimum, a reinspection shall examine the software product areas changed to resolve anomalies identified in the last inspection, as well as side effects of those changes.

6.5.7 Rework/follow-up

The inspection leader shall verify that the action items assigned in the meeting are closed.

6.6 Exit criteria

An inspection shall be considered complete when the activities listed in 6.5 have been accomplished, and the output described in 6.7 exists.

6.7 Output

The output of the inspection shall be documented evidence that identifies the following:

a) The project that created the software product under inspection

b) The inspection team members

c) The inspection meeting duration

d) The software product inspected

e) The size of the materials inspected (for example, the number of text pages)

f) Specific inputs to the inspection

g) Inspection objectives and whether they were met

h) The anomaly list, containing each anomaly location, description, and classification

i) The disposition of the software product

j) Any waivers granted or waivers requested

k) Individual and total preparation time of the inspection team

l) The total rework time

The inspection output should include the following:

m) The inspection anomaly summary listing the number of anomalies identified by each anomaly category

n) An estimate of the rework effort and rework completion date, if the rework effort is expected to be significant

The inspection output may include the following:

o) An estimate of the savings by fixing items found in inspection, compared to their cost to fix if identified later

Although this standard sets minimum requirements for the content of the documented evidence, it is left to local procedures to prescribe additional content, format requirements, and media.

6.8 Data collection

Inspections shall provide data for the analysis of the quality of the software product, the effectiveness of the acquisition, supply, development, operation and maintenance processes, and the effectiveness and the efficiency of the inspection itself. In order to maintain the effectiveness of inspections, data from the author and inspectors shall not be used to evaluate the performance of individuals. To enable these analyses, anomalies that are identified at an inspection meeting shall be classified in accordance with 6.8.1, 6.8.2, and 6.8.3.

Inspection data shall contain the identification of the software product, the date and time of the inspection, the inspection team, the preparation and inspection times, the volume of the materials inspected, and the

disposition of the inspected software product. The capture of this information shall be used to optimize local guidance for inspections.

The management of inspection data requires a capability to enter, store, access, update, summarize, and report classified anomalies. The frequency and types of the inspection analysis reports, and their distribution, are left to local standards and procedures.

6.8.1 Anomaly classification

Classification of software product anomalies shall be accomplished, for example, using IEEE Std 1044-1993 [B8] classification schemes. Anomaly classification facilitates a standard terminology for anomalies within or between projects and organizations. IEEE Std 1044-1993 [B8] defines a number of categories within which anomalies may be classified. The categories a project may select depend on many factors, including software product and life cycle phase.

6.8.2 Anomaly categories

Categories represent various attributes of an anomaly to which groups of classifications belong. Anomaly categories can be representative of when the anomaly was found, its investigation, its impact, resolution activities, and final disposition.

For example, a software documentation nonconformance-type category may include the following classifications:

— Missing

— Extra (superfluous)

— Ambiguous

— Inconsistent

— Not conforming to standards

— Risk-prone, i.e., the review finds that, although an item was not shown to be "wrong," the approach taken involves risks (and there are known safer alternative methods)

— Incorrect

— Unachievable (e.g., because of system, time, or technical constraints)

— Editorial

6.8.3 Anomaly ranking

Anomalies shall be ranked by potential impact on the software product, for example, as follows:

a) *Catastrophic.* Anomalies that would result in software failure with grave consequences, such as loss of life, failure of mission, or very large economic or social loss; mitigation is not possible.

b) *Critical.* Anomalies that would result in software failure with major consequences, such as injury, major system degradation, partial failure of mission, or major economic or social loss; partial to complete mitigation is possible.

c) *Marginal.* Anomalies that would result in software failure with minor consequences; complete mitigation is possible.

d) *Negligible.* Anomalies that would not result in software failure; mitigation is not necessary.

6.9 Improvement

Inspection data shall be analyzed regularly in order to improve the inspection process itself, and should be used to improve the activities used to produce software products. Frequently occurring anomalies shall be included in the inspection checklists or role assignments. The checklists themselves shall also be inspected regularly for superfluous or misleading questions. Consistently granted or requested waivers shall be analyzed to determine if the standards need to be changed. The preparation times, meeting times, and number of participants shall be analyzed to determine connections between preparation (checking) rate, meeting rate, and number and severity of anomalies found. Benefits (savings) achieved should be assessed regularly, and the inspection process should be continually adapted to achieve greater effectiveness at maximum efficiency

7. Walk-throughs

7.1 Introduction to walk-throughs

The purpose of a systematic walk-through is to evaluate a software product. A walk-through may be held for the purpose of educating an audience regarding a software product. The major objectives are as follows:

a) Find anomalies

b) Improve the software product

c) Consider alternative implementations

d) Evaluate conformance to standards and specifications

e) Evaluate the usability and accessibility of the software product

Other important objectives of the walk-through include exchange of techniques, style variations, and training of the participants. A walk-through may point out deficiencies (for example, efficiency and readability problems in the software product, modularity problems in design or code, or untestable specifications).

Examples of software products subject to walk-throughs include, but are not limited to, the following:

— Software requirements specification

— Software design description

— Source code

— Software test plans and procedures

— Software user documentation

— Maintenance manual

— Specifications

— System build procedures

— Installation procedures

— Release notes

— License

— Software development process descriptions

— Software architectural descriptions

7.2 Responsibilities

The following roles shall be established for the walk-through:

a) Walk-through leader

b) Recorder

c) Author

d) Team member

For a review to be considered a systematic walk-through, a team of at least two members (including the author) shall be assembled. Roles may be shared among the team members. The walk-through leader or the author may serve as the recorder. The walk-through leader may be the author.

Individuals holding management positions over any member of the walk-through team shall not participate in the walk-through.

7.2.1 Walk-through leader

The walk-through leader shall conduct the walk-through, shall handle the administrative tasks pertaining to the walk-through (such as distributing documents and arranging the meeting), and shall ensure that the walk-through is conducted in an orderly manner. The walk-through leader shall prepare the statement of objectives to guide the team through the walk-through. The walk-through leader shall ensure that the team arrives at a decision or identified action for each discussion item, and shall issue the walk-through output as described in 7.7.

7.2.2 Recorder

The recorder shall note all decisions and identified actions arising during the walk-through meeting. In addition, the recorder should note all comments made during the walk-through that pertain to anomalies found, questions of style, omissions, contradictions, suggestions for improvement, or alternative approaches.

7.2.3 Author

The author should present the software product in the walk-through.

7.2.4 Team member

Walk-through team members shall adequately prepare for and actively participate in the walk-through. Team members shall identify and describe anomalies in the software product.

7.3 Input

Input to the walk-through shall include the following:

a) A statement of objectives for the walk-through

b) The software product being examined

c) Standards that are in effect for the acquisition, supply, development, operation, and/or maintenance of the software product

Input to the walk-through may also include the following:

d) Any regulations, standards, guidelines, plans, specifications, and procedures against which the software product is to be evaluated

e) Anomaly categories (see IEEE Std 1044-1993 [B8])

f) Walk-through checklists

Additional reference material may be made available by the individuals responsible for the software product when requested by the walk-through leader.

7.4 Entry criteria

7.4.1 Authorization

The need for conducting walk-throughs shall be established in the appropriate project planning documents. Additional walk-throughs may be conducted during acquisition, supply, development, operation, and maintenance of the software product at the request of project management, quality management, or the author, according to local procedures.

7.4.2 Preconditions

A walk-through shall be conducted only when all of the following conditions have been met:

a) A statement of objectives for the review is established.

b) The required review inputs are available.

c) Any standards that are required to evaluate the software product are available.

7.5 Procedures

7.5.1 Management preparation

Managers or persons responsible for the walk-through shall ensure that the walk-through is performed as required by applicable standards and procedures and by requirements mandated by law, contract, or other policy. To this end, they shall do the following:

a) Plan time and resources required for walk-throughs, including support functions, as required in IEEE Std 1058-1987 [B9] or other appropriate standards

b) Provide funding and facilities required to plan, define, execute, and manage the walk-through

c) Provide training and orientation on walk-through procedures applicable to a given project

d) Ensure that walk-through team members possess appropriate levels of expertise and knowledge sufficient to comprehend the software product

e) Ensure that planned walk-throughs are conducted

f) Act on walk-through team recommendations in a timely manner

7.5.2 Planning the walk-through

The walk-through leader shall be responsible for the following activities:

a) Identify the walk-through team

b) Schedule the meeting and select the meeting place

c) Distribute necessary input materials to participants, and allow adequate time for their preparation

7.5.3 Overview

An overview presentation may be made by the author as part of the walk-through meeting.

7.5.4 Preparation

The walk-through leader shall distribute the software product and convene a walk-through meeting. Team members shall prepare for the meeting by examining the software product and preparing a list of items for discussion in the meeting. These items should be divided into two categories: general and specific. General items apply to the whole product; specific items apply to a part of it.

Each walk-through team member shall examine the software product and other review inputs prior to the review meeting. Anomalies detected during this examination shall be documented and sent to the walk-through leader. The walk-through leader should classify anomalies to ensure that walk-through meeting time is used effectively. The walk-through leader should forward the anomalies to the author of the software product for disposition.

The author or walk-through leader shall specify a suitable order in which the software product will be evaluated (such as sequential, hierarchical, data flow, control flow, bottom up, or top down).

7.5.5 Examination

The walk-through leader shall introduce the participants and describe their roles. The walk-through leader shall state the purpose of the walk-through and should act as a facilitator to ensure that everyone has had a chance to comment and should solicit comments from attendees to ensure that all voices are heard. The walk-through leader should remind the team members to comment only on the software product, not its author. Team members may pose questions to the author regarding the software product. The walk-through leader shall resolve any special procedural questions raised by the team members.

The author may present an overview of the software product under review. This should be followed by a general discussion during which team members raise their general items. After the general discussion, the author presents the software product in detail (hence the name “walk-through”) using the order determined as part of preparation. Team members raise their specific items when the author reaches them in the presentation. New items may be raised during the meeting. The walk-through leader coordinates discussion and guides the meeting to a decision or identified action on each item. The recorder notes all recommendations and required actions.

During the walk-through meeting

a) The author or walk-through leader should make an overview presentation of the software product under examination.

b) The walk-through leader shall coordinate a discussion of the general anomalies of concern.

c) The author or walk-through leader shall present the software product, describing every portion of it.

d) Team members shall raise specific anomalies as the author reaches the part of the software product to which the anomalies relate.

e) The recorder shall note recommendations and actions arising out of the discussion upon each anomaly.

After the walk-through meeting, the walk-through leader shall issue the walk-through output detailing anomalies, decisions, actions, and other information of interest. Minimum content requirements for the walk-through output are provided in 7.7.

7.5.6 Rework/follow-up

The walk-through leader shall verify that the action items assigned in the meeting are closed.

7.6 Exit criteria

The walk-through shall be considered complete when

a) The objectives stated in item a) of 7.3 have been met.

b) Recommendations and required actions have been recorded.

c) The walk-through output has been completed.

7.7 Output

The output of the walk-through shall be documented evidence that identifies the following:

a) The project for which the walk-through was performed

b) The walk-through team members

c) The software product being examined

d) The statement of objectives that were to be accomplished during this walk-through meeting and whether they were met

e) The anomaly list, containing each anomaly location and description

f) A list of the recommendations made regarding each anomaly

g) A list of actions, due dates, and responsible people

h) Any recommendations made by the walk-through team on how to dispose of deficiencies and unresolved anomalies

i) Any proposals made by the walk-through team for follow-up walk-throughs

Although this standard sets minimum requirements for the content of the documented evidence, it is left to local procedures to prescribe additional content, format requirements, and media.

7.8 Data collection recommendations

Walk-throughs should provide data for the analysis of the quality of the software product, the effectiveness of the acquisition, supply, development, operation, and maintenance processes, and the efficiency of the walk-through itself. In order to maintain the effectiveness of walk-throughs, data should not be used to evaluate the performance of individuals.

Walk-through data should contain the identification of the software product, the date and time of the walk-through, the walk-through leader, the preparation and walk-through times, the volume of the materials walked through, and the disposition of the software product. The capture of this information can be used to optimize local guidance for walk-throughs.

The management of walk-through data requires a capability to store, enter, access, update, summarize, and report categorized anomalies. The frequency and types of the walk-through analysis reports, and their distribution, are left to local standards and procedures.

Anomalies identified during walk-throughs may be classified in accordance with IEEE Std 1044-1993 [B8].

7.9 Improvement

Walk-through data should be analyzed regularly in order to improve the walk-through process itself and to improve the software activities used to produce the software product. Frequently occurring anomalies may be included in the walk-through checklists or role assignments. The checklists themselves should also be evaluated regularly for superfluous or misleading questions. The preparation times, meeting times, and number of participants should be analyzed to determine connections between preparation rate, meeting rate, and number and severity of anomalies found.

8. Audits

8.1 Introduction to audits

The purpose of a software audit is to provide an independent evaluation of conformance of software products and processes to applicable regulations, standards, guidelines, plans, specifications, and procedures.

Examples of software products subject to audit include, but are not limited to, the following:

- Backup and recovery plans
- Contingency plans
- Contracts
- Customer or user representative complaints
- Disaster plans
- Hardware performance plans
- Installation plans
- Installation procedures
- Maintenance plans
- Management review reports
- Operations and user manuals
- Procurement and contracting methods
- Reports and data (for example, review, audit, project status, anomaly reports, test data)
- Request for proposal
- Risk management plans
- Software configuration management plans (see IEEE Std 828-2005 [B3])
- Software design descriptions (see IEEE Std 1016-1998 [B7])
- Source code

— Unit development folders
— Software project management plans (see IEEE Std 1058-1998 [B9])
— Software quality assurance plans (see IEEE Std 730-2002 [B2])
— Software requirements specifications (see IEEE Std 830-1998 [B5])
— Software safety plans (see IEEE Std 1228-1994 [B13])
— Software test documentation (see IEEE Std 829-2008 [B4])
— Software user documentation (see IEEE Std 1063-2001 [B10])
— Software verification and validation plans (see IEEE Std 1012-2004 [B6])
— Software architectural descriptions (see IEEE Std 1471-2000 [B14])
— Standards, regulations, guidelines, plans, specifications, and procedures
— System build procedures
— Technical review reports
— Vendor documents
— Walk-through reports
— Deliverable media (such as tapes and diskettes)

Examples of software processes subject to audit include, but are not limited to, software development life cycle process descriptions

The examination should begin with an opening meeting during which the auditors and audited organization examine and agree upon the arrangements for the audit.

When stipulated in the audit plan, the auditors may make recommendations. These should be reported separately.

8.2 Responsibilities

The following roles shall be established for an audit:

a) Lead auditor
b) Recorder
c) Auditor(s)
d) Initiator
e) Audited organization

The lead auditor may act as recorder. The initiator should not act as lead auditor. Additional auditors should be included in the audit team; however, audits by a single person are permitted.

8.2.1 Lead auditor

The lead auditor shall be responsible for the audit. This responsibility includes administrative tasks pertaining to the audit, ensuring that the audit is conducted in an orderly manner, and ensuring that the audit meets its objectives. The lead auditor is responsible for the following:

a) Preparing the audit plan (see 8.5.2)

b) Assembling the audit team

c) Managing the audit team

d) Making decisions regarding the conduct of the audit

e) Making decisions regarding any audit observations

f) Preparing the audit report (see 8.7)

g) Reporting on the inability or apparent inability of any of individuals involved in the audit to fulfill their responsibilities

h) Negotiating any discrepancies or inconsistencies with the initiator which could impair the ability to satisfy the exit criteria (see 8.6)

i) Recommending corrective actions

The lead auditor shall be free from bias and influence that could reduce the ability to make independent, objective evaluations.

8.2.2 Recorder

The recorder shall document anomalies, action items, decisions, and recommendations made by the audit team.

8.2.3 Auditor

The auditors shall examine products, as defined in the audit plan. They shall document their observations. All auditors shall be free from bias and influences that could reduce their ability to make independent, objective evaluations, or they shall identify their bias and proceed with acceptance from the initiator.

8.2.4 Initiator

The initiator shall be responsible for the following activities:

a) Decide upon the need for an audit

b) Decide upon the purpose and scope of the audit

c) Decide the software products or processes to be audited

d) Decide the evaluation criteria, including the regulations, standards, guidelines, plans, specifications, and procedures to be used for evaluation

e) Decide who will carry out the audit

f) Review the audit report

g) Decide what follow-up action will be required

h) Distribute the audit report

The initiator may be a manager in the audited organization, a customer or user representative of the audited organization, or a third party.

8.2.5 Audited organization

The audited organization shall provide a liaison to the auditors and shall provide all information requested by the auditors. When the audit is completed, the audited organization should implement corrective actions and recommendations.

8.3 Input

Inputs to the audit shall be listed in the audit plan and shall include the following:

a) Purpose and scope of the audit

b) Background information about the audited organization

c) Software products or processes to be audited

d) Evaluation criteria, including applicable regulations, standards, guidelines, plans, specifications, and procedures to be used for evaluation

e) Impact criteria (for example, “acceptable,” “needs improvement,” “unacceptable,” “not rated”)

Inputs to the audit should also include the following:

f) Records of previous similar audits

Additional reference material may be made available by the individuals responsible for the software product or process when requested by the audit leader.

8.4 Entry criteria

8.4.1 Authorization

An initiator decides upon the need for an audit. This decision may be prompted by a routine event, such as the arrival at a project milestone, or a non-routine event, such as the suspicion or discovery of a major non-conformance.

The initiator selects an auditing organization that can perform an independent evaluation. The initiator provides the auditors with information that defines the purpose of the audit, the software products or processes to be audited, and the evaluation criteria. The initiator should request the auditors to make recommendations. The lead auditor produces an audit plan, and the auditors prepare for the audit.

The need for an audit may be established by one or more of the following events:

a) The supplier organization decides to verify compliance with the applicable regulations, standards, guidelines, plans, specifications, and procedures (this decision may have been made when planning the project).

b) The customer organization decides to verify compliance with applicable regulations, standards, guidelines, plans, specifications, and procedures.

c) A third party, such as a regulatory agency or assessment body, decides upon the need to audit the supplier organization to verify compliance with applicable regulations, standards, guidelines, plans, specifications, and procedures.

In every case, the initiator shall authorize the audit.

8.4.2 Preconditions

An audit shall be conducted only when all of the following conditions have been met:

a) The audit has been authorized by an appropriate authority.

b) A statement of objectives of the audit is established.

c) The required audit inputs are available.

8.5 Procedures

8.5.1 Management preparation

Managers shall ensure that the audit is performed as required by applicable standards and procedures and by requirements mandated by law, contract, or other policy. To this end, managers shall do the following:

a) Plan time and resources required for audits, including support functions, as required in IEEE Std 1058-1998 [B9], legal or regulatory documents, or other appropriate standards

b) Provide funding and facilities required to plan, define, execute, and manage the audits

c) Provide training and orientation on the audit procedures applicable to a given project

d) Ensure appropriate levels of expertise and knowledge sufficient to comprehend the software product being audited

e) Ensure that planned audits are conducted

f) Act on audit team recommendations in a timely manner

8.5.2 Planning the audit

The audit plan shall describe the following:

a) Purpose and scope of the audit

b) Audited organization, including location and management

c) Software products to be audited

d) Evaluation criteria, including applicable regulations, standards, guidelines, plans, specifications, and procedures to be used for evaluation

e) Auditor's responsibilities

f) Examination activities (for example, interview staff, read and evaluate documents, observe tests)

g) Audit activity resource requirements

h) Audit activity schedule

i) Requirements for confidentiality (for example, company confidential, restricted information, classified information)

j) Checklists

k) Report formats

l) Report distribution

m) Required follow-up activities

Where sampling is used, a statistically valid sampling method shall be used to establish selection criteria and sample size.

The audit plan shall be approved by the initiator. The audit plan should allow for changes based on information gathered during the audit, subject to approval by the initiator.

8.5.3 Opening meeting

An opening meeting between the audit team and audited organization shall occur at the beginning of the examination phase of the audit. The opening meeting agenda shall include the following:

a) Purpose and scope of the audit

b) Software products or processes being audited

c) Audit procedures and outputs

d) Expected contributions of the audited organization to the audit (for example, the number of people to be interviewed, meeting facilities)

e) Audit schedule

f) Access to facilities, information, and documents required

8.5.4 Preparation

The initiator shall notify the audited organization's management in writing before the audit is performed, except for unannounced audits. The notification shall define the purpose and scope of the audit, identify what will be audited, identify the auditors, and identify the audit schedule. The purpose of notification is to enable the audited organization to ensure that the people and material to be examined in the audit are available.

Auditors shall prepare for the audit by studying the following:

a) Audit plan

b) Audited organization

c) Products or processes to be audited

d) Applicable regulations, standards, guidelines, plans, specifications, and procedures to be used for evaluation

e) Evaluation criteria

In addition, the lead auditor shall make the necessary arrangements for the following:

f) Team orientation and training

g) Materials, documents, and tools required by the audit procedures

h) Examination activities

8.5.5 Examination

Examination shall consist of evidence collection and analysis with respect to the audit criteria, a closing meeting between the auditors and audited organization, and preparing an audit report.

8.5.5.1 Evidence collection

The auditors shall collect evidence of conformance and non-conformance by interviewing audited organization staff, examining documents, and witnessing processes. The auditors should attempt all the examination activities defined in the audit plan. They shall undertake additional investigative activities if they consider such activities required to define the full extent of conformance or non-conformance.

Auditors shall document all observations of non-conformance and exemplary conformance. An observation is a statement of fact made during an audit that is substantiated by objective evidence. Examples of non-conformance are as follows:

— Applicable regulations, standards, guidelines, plans, specifications, and procedures not used at all

— Applicable regulations, standards, guidelines, plans, specifications, and procedures not used correctly

Observations should be categorized as major or minor. An observation should be classified as major if the non-conformity will likely have a significant effect on product quality, project cost, or project schedule. Major observations are frequently termed "findings."

All observations shall be verified by discussing them with the audited organization before the closing audit meeting.

8.5.5.2 Closing meeting

The lead auditor shall convene a closing meeting with the audited organization's management. The closing meeting should review the following:

a) Actual extent of implementation of the audit plan

b) Problems experienced in implementing the audit plan, if any

c) Observations made by the auditors

d) Preliminary conclusions of the auditors

e) Preliminary recommendations of the auditors

f) Overall audit assessment (for example, whether the audited organization successfully passed the audit criteria)

Comments and issues raised by the audited organization should be resolved. Agreements should be reached during the closing audit meeting and should be completed before the audit report is finalized.

8.5.5.3 Reporting

The lead auditor shall prepare the audit report, as described in 8.7. The audit report should be prepared as soon as possible after the audit. Any communication between auditors and the audited organization made between the closing meeting and the issue of the report should pass through the lead auditor.

The lead auditor shall send the audit report to the initiator and to the audited organization. The initiator should distribute the audit report within the audited organization.

8.5.6 Follow-up

Rework, if any, shall be the responsibility of the initiator and audited organization and shall include the following:

a) Determining what corrective action is required to remove or prevent a non-conformity

b) Initiating the corrective action

8.6 Exit criteria

An audit shall be considered complete when

a) The audit report has been submitted to the initiator.

b) All of the auditing organization's findings included in the scope of the audit are opened or resolved and approved closed.

8.7 Output

The output of the audit is the audit report. The audit report shall contain the following:

a) Purpose and scope of the audit

b) Audited organization, including location, liaison staff, and management

c) Identification of the software products or processes audited

d) Applicable regulations, standards, guidelines, plans, specifications, and procedures used for evaluation

e) Evaluation criteria

f) Summary of auditor's organization

g) Summary of examination activities

h) Summary of the planned examination activities not performed

i) Observation list, classified as major (finding) or minor

j) A summary and interpretation of the audit findings including the key items of non-conformance

k) The type and timing of audit follow-up activities

Additionally, when stipulated by the audit plan, recommendations shall be provided to the audited organization or the initiator. Recommendations may be reported separately from results.

Although this standard sets minimum requirements for report content, it is left to local standards to prescribe additional content, report format requirements, and media.

Annex A

(informative)

Comparison of review types

Table A.1 compares the five types of reviews in a number of salient characteristics. This is meant to be indicative of the ways in which the review types match with or differ from one another.

Table A.1—Comparison of review types

Characteristic	Management review	Technical review	Inspection	Walk-through	Audit
Objective	Monitor progress; set, confirm, or change objectives; change the allocation of resources	Evaluate conformance to specifications and plans; assess change integrity	Find anomalies; verify resolution; verify product quality	Find anomalies; examine alternatives; improve product; forum for learning	Independently evaluate conformance with objective standards and regulations
Decision-making	Management team charts course of action; decisions made at the meeting or as a result of recommendations	Review team requests management or technical leadership to act on recommendations	Review team chooses predefined product dispositions; anomalies should be removed	The team agrees on changes to be made by the author	Audited organization, initiator, acquirer, customer, or user
Change verification	Leader verifies that action items are closed; change verification left to other project controls	Leader verifies that action items are closed; change verification left to other project controls	Leader verifies that action items are closed; change verification left to other project controls	Leader verifies that action items are closed; change verification left to other project controls	Responsibility of the audited organization
Recommended group size	Two or more people	Three or more people	Three to six people	Two to seven people	One to five people
Group attendance	Management, technical leadership, and documented attendance	Technical leadership and peer mix; documented attendance	Peers meet with documented attendance	Technical leadership and peer mix; documented attendance	Auditors; the audited organization may be called upon to provide evidence
Group leadership	Usually the responsible manager	Usually the lead engineer	Trained facilitator	Facilitator or author	Lead auditor
Volume of material	Moderate to high, depending on the specific meeting objectives	Moderate to high, depending on the specific meeting objectives	Relatively low—whatever can be inspected in a single day; large volumes are subdivided	Relatively low	Moderate to high, depending on the specific audit objectives
Presenter	The review leader determines the presenters	The review leader determines the presenters	A reader	Author	Auditors collect and examine information provided by audited organization

Table A.1—Comparison of review types (continued)

Characteristic	Management review	Technical review	Inspection	Walk-through	Audit
Data collection	As required by applicable policies, standards, or plans	Not a formal project requirement. May be done locally.	Required	Recommended	Not a formal project requirement. May be done locally.
Output	Management review documentation; including the specification of action items, with responsibilities and dates for resolution	Technical review documentation, including the specification of action items, with responsibilities and dates for resolution	Anomaly list, anomaly summary, inspection documentation	Anomaly list, action items, decisions, follow-up proposals	Formal audit report; observations, findings, deficiencies
Formal facilitator training	Yes, usually limited to the review leader	Yes, usually limited to the review leader	Yes, for all participants	Yes, usually limited to the walk-through leader	Yes (formal auditing training)
Defined participant roles	Yes	Yes	Yes	Yes	Yes
Use of anomaly checklists	Optional	Optional	Yes	Optional	Usually no
Management participates	Yes	When management evidence or resolution may be required	No	No	No; however management may be called upon to provide evidence
Customer or user representative participates	Optional	Optional	Optional	Optional	No, however the customer or user representative may be asked to provide evidence

Annex B

(informative)

Bibliography

[B1] IEEE 100™, *The Authoritative Dictionary of IEEE Standards Terms,* Seventh Edition. New York: Institute of Electrical and Electronics Engineers, Inc.[6, 7]

[B2] IEEE Std 730™-2002, IEEE Standard for Software Quality Assurance Plans.

[B3] IEEE Std 828™-2005, IEEE Standard for Software Configuration Management Plans.

[B4] IEEE Std 829™-2008, IEEE Standard for Software Test Documentation.

[B5] IEEE Std 830™-1998, IEEE Recommended Practice for Software Requirements Specifications.

[B6] IEEE Std 1012™-2004, IEEE Standard for Software Verification and Validation.

[B7] IEEE Std 1016™-1998, IEEE Recommended Practice for Software Design Description.

[B8] IEEE Std 1044™-1993, IEEE Standard Classification for Software Anomalies.

[B9] IEEE Std 1058™-1998, IEEE Standard for Software Project Management Plans.

[B10] IEEE Std 1063™-2001, IEEE Standard for Software User Documentation.

[B11] IEEE Std 1074™-2006, IEEE Standard for Developing a Software Life Cycle Process.

[B12] IEEE Std 1220™-2005, IEEE Standard for Application and Management of the Systems Engineering Process.

[B13] IEEE Std 1228™-1994, IEEE Standard for Software Safety Plans.

[B14] IEEE Std 1471™-2000, Systems and Software Engineering—Recommended Practice for Architectural Description of Software-Intensive Systems.

[B15] IEEE Std 12207™-2008, Systems and software engineering—Software life cycle processes.[8]

[B16] IEEE Std 14764™-2006, Standard for Software Engineering—Software Life Cycle Processes—Maintenance.

[B17] ISO 9001:2000, Quality management systems—Requirements.[9]

[B18] ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing.

[B19] ISO/IEC 90003:2004, Software engineering—Guidelines for the application of ISO 9001:2000 to computer software.

[6] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).
[7] The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.
[8] IEEE Std 12207-2008 is also known as ISO/IEC 12207:2008.
[9] ISO publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iso.ch/). ISO publications are also available in the United States from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).