



DPC: 25/30491971 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 21 February 2025

Origin: International

Latest date for receipt of comments: 16 April 2025

Project No. 2024/01250

Responsible committee: IST/15/-/26 Software Testing

Interested committees:

Title: Draft BS ISO/IEC/IEEE 23612 ISO/IEC/IEEE 23612 Software and systems engineering. Incident management.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 16 April 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC/IEEE DIS 23612

Software and systems engineering — Incident management

ICS: 35.080

ISO/IEC JTC 1/SC 7

Secretariat: **BIS**

Voting begins on:
2025-02-21

Voting terminates on:
2025-05-16

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC/IEEE DIS 23612:2025(en)

Full document details: 25/30491971 DC

© ISO/IEC 2025
© IEEE 2025



Documents

Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

© IEEE 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or IEEE at the respective address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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

Email: stds.ipr@ieee.org
Website: www.ieee.org

Contents

Page

Foreword.....iv

Introduction.....v

1 Scope.....1

2 Normative references.....1

3 Terms and definitions.....1

4 Conformance.....2

 4.1 Intended usage.....2

 4.2 Full conformance.....2

 4.3 Tailored conformance.....2

5 Incident management process.....3

 5.1 Overview.....3

 5.2 Purpose.....4

 5.3 Outcomes.....4

 5.4 Activities and tasks.....5

 5.4.1 General.....5

 5.4.2 Plan incident management (IM1).....5

 5.4.3 Raise incident (IM2).....5

 5.4.4 Confirm incident (IM3).....6

 5.4.5 Analyse and decide response (IM4).....6

 5.4.6 Resolve incident (IM5).....6

 5.4.7 Monitor resolution (IM6).....7

 5.4.8 Close incident (IM7).....7

 5.4.9 Report on incidents (IM8).....7

 5.4.10 Incident analysis and improvement (IM9).....8

 5.5 Information items.....8

Annex A (informative) Incident states.....9

Annex B (informative) Incident management data collection.....13

Annex C (normative) Incident documentation templates.....15

Annex D (informative) Incident documentation examples.....24

Annex E (informative) Incident severity and priority.....33

Annex F (informative) Incident management measures.....36

Annex G (informative) Creating incident report titles.....37

Bibliography.....39

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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 contained in its standards.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC1, Information technology, Subcommittee SC 7, Software and systems engineering.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The purpose of this international standard is to define a generic process for incident management that can be used by any organization when performing any form of software and systems development, testing or operations. The processes defined in this document can be used in conjunction with any development life cycle model (e.g. incremental, waterfall, evolutionary, agile).

Software and systems engineering — Incident management

1 Scope

This document defines an incident management process and supporting documentation that can be used to implement incident management and to manage incidents within most organizations, projects or operations activities for a system, service, software, or product. Supporting informative diagrams describing the process and example documents are also provided.

This document is applicable to incident management in all life cycle models (e.g. incremental, waterfall, evolutionary, agile).

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>
- IEEE Standards Dictionary Online: available at: <http://dictionary.ieee.org>

3.1 defect

imperfection or deficiency in a work product where that work product does not meet its requirements or specifications

Note 1 to entry: Requirements can be undocumented.

3.2 incident

anomalous or unexpected event, set of events, condition, or situation at any time during the life cycle of a project, product, service, or system

[SOURCE: ISO/IEC/IEEE 15288:2023, 3.17, note to entry is deleted.]

3.3 incident management

process of recognizing, logging, investigating, classifying, and acting on *incidents* (3.2), and recovery to the normal state

3.4 incident report

documentation of the occurrence, nature and status of an *incident* (3.2)

Note 1 to entry: Incident reports are also known as anomaly reports, bug reports, defect reports, error reports, and trouble reports, amongst other terms.

[SOURCE: ISO/IEC/IEEE 29119-3:2021, 3.4, modified note to remove problem reports and issues]

3.5

incident management report

documentation summarizing the occurrence, nature and status of recorded *incidents* (3.2) over a specified period

3.6

priority

degree of urgency to resolve an incident or an underlying *problem* (3.7), based on its impact to the stakeholders as well as the cost and risk of the fix

Note 1 to entry: The priority is time-variant, as it is dependent on the current phase of the project life cycle

3.7

problem

cause of one or more actual or potential incidents

[SOURCE: ISO/IEC 20000-10:2018, 3.2.10]

3.8

severity

degree of impact that an incident or underlying problem has on the development, testing or operation of a system, software or product

4 Conformance

4.1 Intended usage

The requirements in this document are contained in [Clause 5](#) and [Annex C](#).

This document provides requirements for an incident management process and associated documentation suitable for use during the life cycle of a system, service, software or product. It is recognized that particular projects or organizations may not need to use the complete process defined by this document. Therefore, implementation of this document typically involves selecting a set of activities suitable for the software and systems development, testing or operations. There are two ways that an organization can claim to conform to the provisions of this document.

The organization shall assert whether it is claiming full or tailored conformance to this document.

4.2 Full conformance

Full conformance is achieved by demonstrating that all of the requirements (i.e. shall statements) of the process defined in [Clause 5](#) and the test documentation defined in [Annex C](#) have been met.

4.3 Tailored conformance

When this document is used as a basis for establishing an incident management process that does not qualify for full conformance, the subset of activities for which tailored conformance is claimed, is recorded. Tailored conformance is achieved by demonstrating that all of the requirements (i.e. shall statements) for the recorded subset of activities have been satisfied.

When this document is used as a basis for establishing a set of incident management documentation that does not qualify for full conformance, the subset of documentation for which tailored conformance is claimed, shall be recorded. Tailored conformance is achieved by demonstrating that all requirements (i.e. shall statements) for the recorded subset of incident management documentation defined in [Annex C](#) have been satisfied.

Where tailoring occurs, justification shall be provided (either directly or by reference), whenever an activity defined in [Clause 5](#) is not followed or the requirements of incident management documentation are not met.

All tailoring decisions shall be recorded with their rationale, including the consideration of any applicable risks. Tailoring decisions shall be agreed by the relevant stakeholders.

EXAMPLE Where organizations follow information item management processes in standards such as ISO 15489-1, ISO 9001, ISO/IEC 20000-1 or use similar internal organizational processes, they can decide to use those processes in place of the information item management tasks defined in this document.

5 Incident management process

5.1 Overview

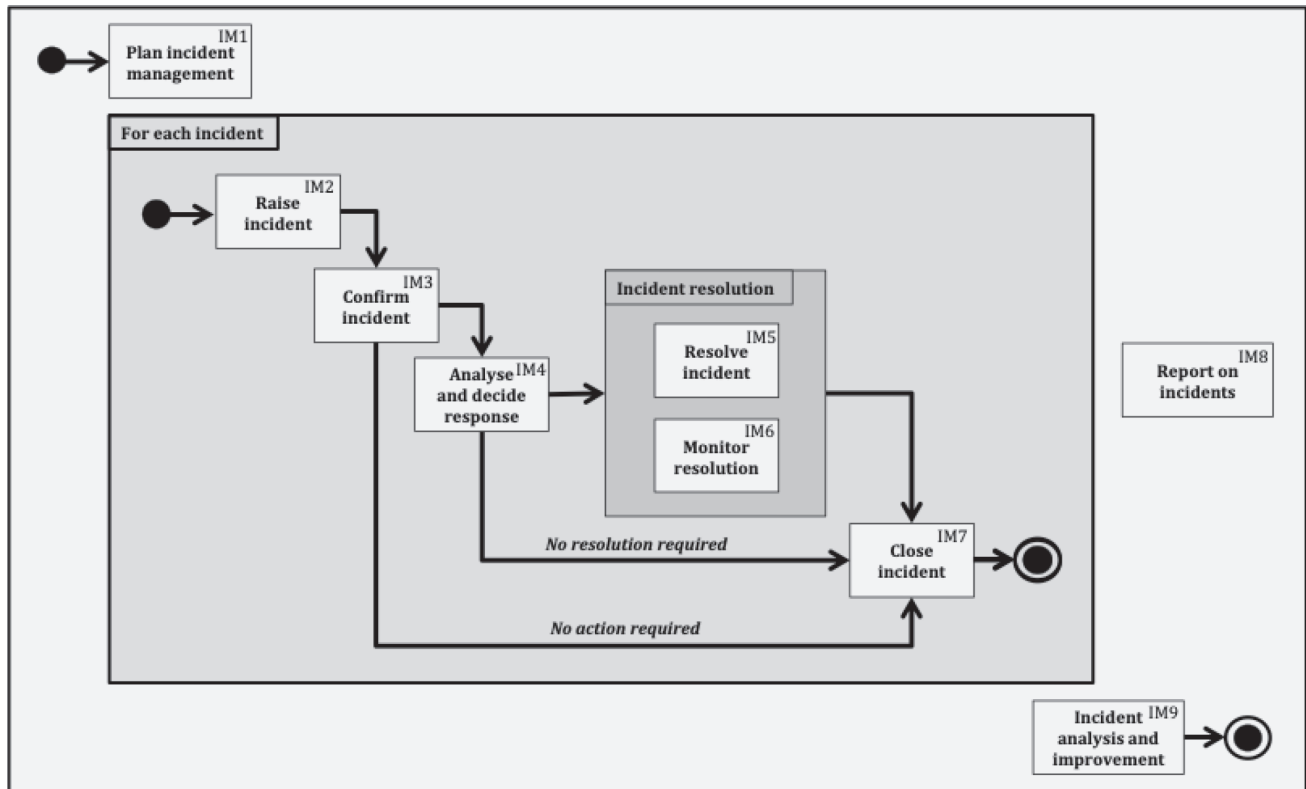
The incident management process shown in [Figure 1](#) is used to both manage the set of incidents identified across a project, a service or organization (see IM1, IM8 and IM9 in [Figure 1](#)), and individual incidents from their occurrence to their closure (see IM2 to IM7 in [Figure 1](#)).

Incident management includes planning how incidents are to be handled by a project or organization (the first activity, IM1, in [Figure 1](#)), reporting on the status of these incidents (IM8 in [Figure 1](#)), and how these incidents are analysed to improve subsequent performance in the project or organization (the final activity, IM9, in [Figure 1](#)). The core of this process (IM2 to IM7 in [Figure 1](#)) is formed by the activities for managing individual incidents, in which some activities can be combined, for instance, if the project is small. As each individual incident progresses through this process, it will pass through several states, such as raised, confirmed, under resolution and closed. Possible states and the possible transitions between them are shown in the state models provided in [Annex A](#).

Incidents can be raised at any point in the life cycle of the system, software or product, and can be as a result of operational use, review, development or testing activities. Incident management can result in the correction of defects or the improvement of the product, as well as improvements to the processes by which the system is used, developed, reviewed, or tested.

The incident management process is often specified as part of a generic incident management plan, which could be defined as an organizational practice, that can be applied to all projects in an organization. In some situations this will require the generic plan to be customized for individual projects. Ideally any customization will still allow the comparison of incident management measures from different projects and the sharing of potential improvements to the implemented processes. Typical inputs to this process include:

- previous/current incident management processes; and
- current development, verification, validation, test and operational practices.



NOTE Some of the activities in this figure are often combined in practice for smaller projects, organizations or systems.

Figure 1 — Incident management process

5.2 Purpose

The purpose of the incident management process is to manage all incidents to resolution.

When managing incidents at a high level (e.g. organization or project level), the incident management process is planned and agreed, and the information gathered from reported incidents is used to improve the relevant processes.

When an individual incident requires a response, the work is assigned to a suitable party for resolution, and the resolution activities are monitored for acceptability. Once the resolution is approved, then the incident is closed, and the incident management process for that individual incident is deemed complete.

5.3 Outcomes

As a result of the successful implementation of the incident management process:

- The incident management plan is agreed.
- Incidents are raised and confirmed.
- Incidents are analysed and assigned for response.
- Incidents are resolved.
- Incident resolution is monitored.
- The resolution of incidents is verified, and the incidents are closed.
- Incident report data is collected to be used for future analysis.

- h) Incidents are analysed, and improvements actioned.

5.4 Activities and tasks

5.4.1 General

The personnel responsible for incident management will implement the following activities and tasks in accordance with applicable organization policies and procedures with respect to the incident management process.

5.4.2 Plan incident management (IM1)

This activity consists of the following tasks:

- a) The process for managing individual incidents:
 - 1) shall be defined;
 - 2) shall be recorded in the incident management plan;
 - 3) shall be agreed by the relevant stakeholders.
 - 4) shall be communicated to the relevant stakeholders as part of the incident management plan.

EXAMPLE Stakeholders can include head of quality assurance, head of development, head of testing and head of service management.

NOTE This group of stakeholders can include anyone who takes part in the incident management process, such as those who are expected to confirm and analyse incidents, those who decide responses, and those who resolve incidents and check their resolution.

- b) The process for analysing incidents to identify potential improvements:
 - 1) should be defined;
 - 2) should be recorded;
 - 3) should be agreed by the relevant stakeholders.
 - 4) should be communicated to the relevant stakeholders as part of the incident management plan.

5.4.3 Raise incident (IM2)

This activity consists of the following tasks:

- a) Details of the incident shall be recorded as part of an incident report, including a status indicating that it has been raised.

NOTE 1 Incidents can be raised by a wide variety of stakeholders, such as users, testers and developers, or automatically by an autonomous system (see [D.3.3](#)).

NOTE 2 At this point in the incident management process, only a subset of the fields in the incident report can be completed. [Annex B](#) shows the typical incident information collected at various points in the incident management process.

- b) The incident report shall be communicated to the relevant stakeholders as detailed in the incident management plan.

EXAMPLE Mechanisms for reporting and communicating incidents include through an incident management tool, on paper to the relevant person or team, or through a test management tool.

5.4.4 Confirm incident (IM3)

This activity consists of the following tasks:

- a) The incident shall be evaluated to confirm whether it requires further action.

NOTE 1 In larger organizations, this activity is sometimes handled by a team responsible for handling incidents, such as a defect triage team or service desk.

- b) If further action is required:

- 1) the incident report shall be updated to reflect the result of the evaluation;
- 2) the incident status shall be communicated to relevant stakeholders;
- 3) the incident shall be assigned to a person or team with the relevant expertise, time and skills to perform an effective analysis of the incident;
- 4) the incident shall be progressed to the analyse and decide response activity ([5.4.5](#)).

NOTE 2 If the reported incident appears to be a duplicate of a previously raised incident, the two incident reports are usually linked together.

- c) If no further action is required:

- 1) the incident report should be updated with the justification for its closure;
- 2) the incident shall be progressed to the close incident activity ([5.4.8](#)).

5.4.5 Analyse and decide response (IM4)

This activity consists of the following tasks:

- a) The incident shall be analysed to gather sufficient information to determine if it requires resolution, or not.

- b) If the incident requires resolution:

- 1) the incident shall be assigned to a person or team for resolution;
- 2) the incident shall be progressed to the resolve incident activity ([5.4.6](#));
- 3) a person or team should be assigned to monitor its resolution as part of the monitor resolution activity ([5.4.7](#));
- 4) the incident report shall be updated with resolution information.

EXAMPLE Resolution information typically includes expectations such as the target version for the response, reporting requirements, and acceptance criteria.

- c) If the incident does not require resolution:

- 1) the incident report should be updated with the justification for its closure;
- 2) the incident shall be progressed to the close incident activity ([5.4.8](#)).

5.4.6 Resolve incident (IM5)

This activity consists of the following tasks:

- a) Corrective actions to resolve the incident shall be performed.

NOTE 1 Sometimes the person or team assigned to perform incident resolution will find that they cannot resolve the incident due to various factors, such as time or effort constraints, lack of available skills or tools, the inability to recreate the incident, or a misunderstanding about the functionality, in which case the incident is returned to the analyse and decide response activity ([5.4.5](#)).

- b) The changes made should be tested to provide confidence that the corrective actions successfully addressed the incident.

NOTE 2 If the corrective actions failed to successfully address the incident, the incident report is updated to include any additional useful information gathered about the incident and further corrective actions are performed by returning to task a).

NOTE 3 In some circumstances testing will not be necessary, such as when the change is fixing a typographical error.

- c) The incident report shall be updated to reflect the corrective actions taken and testing performed.

NOTE 4 Some corrective actions will have an effect on other artefacts, such as other subsystems or systems.

- d) The result of the incident resolution and the status of the incident shall be communicated to relevant stakeholders.

NOTE 5 During development, corrective actions are normally the responsibility of the development team, while, once operational, the corrective actions often become the responsibility of a maintenance team.

5.4.7 Monitor resolution (IM6)

This activity consists of the following tasks:

- a) The timeliness of the corrective actions and the success of these actions against the acceptance criteria should be monitored by a person or team independent of those implementing the actions.
- b) Where necessary, actions to support successful incident resolution should be taken.

EXAMPLE 1 The provision of additional resources or the re-assignment of the incident resolution to a different person or team.

- c) Once the corrective actions are reported as completed, the results shall be checked to confirm that the incident has been successfully resolved.

EXAMPLE 2 Checking test results, or re-running confirmation and regression tests.

- d) The incident report shall be updated to reflect the resolution result and the target build/version.
- e) Resolved incidents shall be progressed to the close incident activity ([5.4.8](#)).
- f) Unresolved incidents shall either be returned to the resolve incident activity ([5.4.6](#)) for additional resolution actions or to the analyse and decide response activity ([5.4.5](#)) for further analysis to decide an alternative response.

5.4.8 Close incident (IM7)

This activity consists of the following tasks:

- a) The incident report shall be updated to reflect approval that the incident has been addressed and the incident status is changed to closed.
- b) A closure reason should be recorded for each incident, to support future incident analysis and improvement activities.
- c) The incident report should be stored for subsequent analysis in the incident analysis and improvement activity ([5.4.10](#)).

5.4.9 Report on incidents (IM8)

This activity consists of the following tasks:

- a) The collective status of reported incidents shall be determined.