International Standard

ISO/IEC/IEEE 23612

Software and systems engineering — Incident management

Ingénierie du logiciel et des systèmes — Gestion d'incident

First edition
2026-05

Reference number
ISO/IEC/IEEE 23612:2026(en)

COPYRIGHT PROTECTED DOCUMENT

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

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

Published in Switzerland

Contents

Page

Foreword ... **iv**

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 ... 5
5.3 Outcomes ... 5
5.4 Activities and tasks ... 5
5.4.1 General ... 5
5.4.2 Plan and implement incident management (IM1) ... 5
5.4.3 Raise incident (IM2) ... 6
5.4.4 Confirm incident (IM3) ... 6
5.4.5 Analyse and decide response (IM4) ... 6
5.4.6 Resolve incident (IM5) ... 7
5.4.7 Confirm resolution (IM6) ... 7
5.4.8 Close incident (IM7) ... 8
5.4.9 Monitor and report on incidents (IM8) ... 8
5.4.10 Incident analysis and improvement (IM9) ... 8
5.5 Information items ... 8

Annex A (informative) **Incident states** ... **10**

Annex B (informative) **Incident management data collection** ... **15**

Annex C (normative) **Incident documentation templates** ... **17**

Annex D (informative) **Incident documentation examples** ... **26**

Annex E (informative) **Incident severity and priority** ... **28**

Annex F (informative) **Incident management measures** ... **31**

Annex G (informative) **Creating incident report titles** ... **32**

Bibliography ... **34**

IEEE notices and abstract ... **35**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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 or www.iec.ch/members_experts/refdocs).

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, 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.

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*, in cooperation with the Systems and Software Engineering Standards Committee of the IEEE Computer Society, under the Partner Standards Development Organization cooperation agreement between ISO and IEEE.

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 and www.iec.ch/national-committees.

Software and systems engineering — Incident management

1 Scope

This document defines a generic 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. This document also provides supporting diagrams describing the process and example documents.

This document is applicable to incident management in all life cycle models (e.g. incremental, waterfall, evolutionary, agile). This document covers incidents identified across the life cycle, including those that arise during both development (e.g. defects) and operation (e.g. those handled by service management).

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, IEC and IEEE 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

NOTE Definitions for other systems and software engineering terms typically can be found in ISO/IEC/IEEE 24765, available at www.computer.org/sevocab.

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 are not always documented and can contain defects.

[SOURCE: ISO/IEC/IEEE 32675:2022, 3.1, modified — The words ‘or characteristic’ have been removed; the words "where" and "work product" have been added; note 1 to entry has been added.]

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, modified — Note 1 to entry has been 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* (3.1) reports, error reports, and trouble reports, amongst other terms.

[SOURCE: ISO/IEC/IEEE 29119-3:2021, 3.4, modified — In note 1 to entry, "issues" and "problem reports" have been removed.]

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* (3.2) 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* (3.2)

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

3.8
severity
degree of impact that an *incident* (3.2) or underlying *problem* (3.7) has on the development, testing or operation of a system, software or product

4 Conformance

4.1 Intended usage

The incident management process shall be in accordance with Clause 5. The test documentation shall be in accordance with Annex C.

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 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 shall be recorded. Tailored conformance is achieved by demonstrating that all of the requirements 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 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 for incident management documentation in Annex C 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).

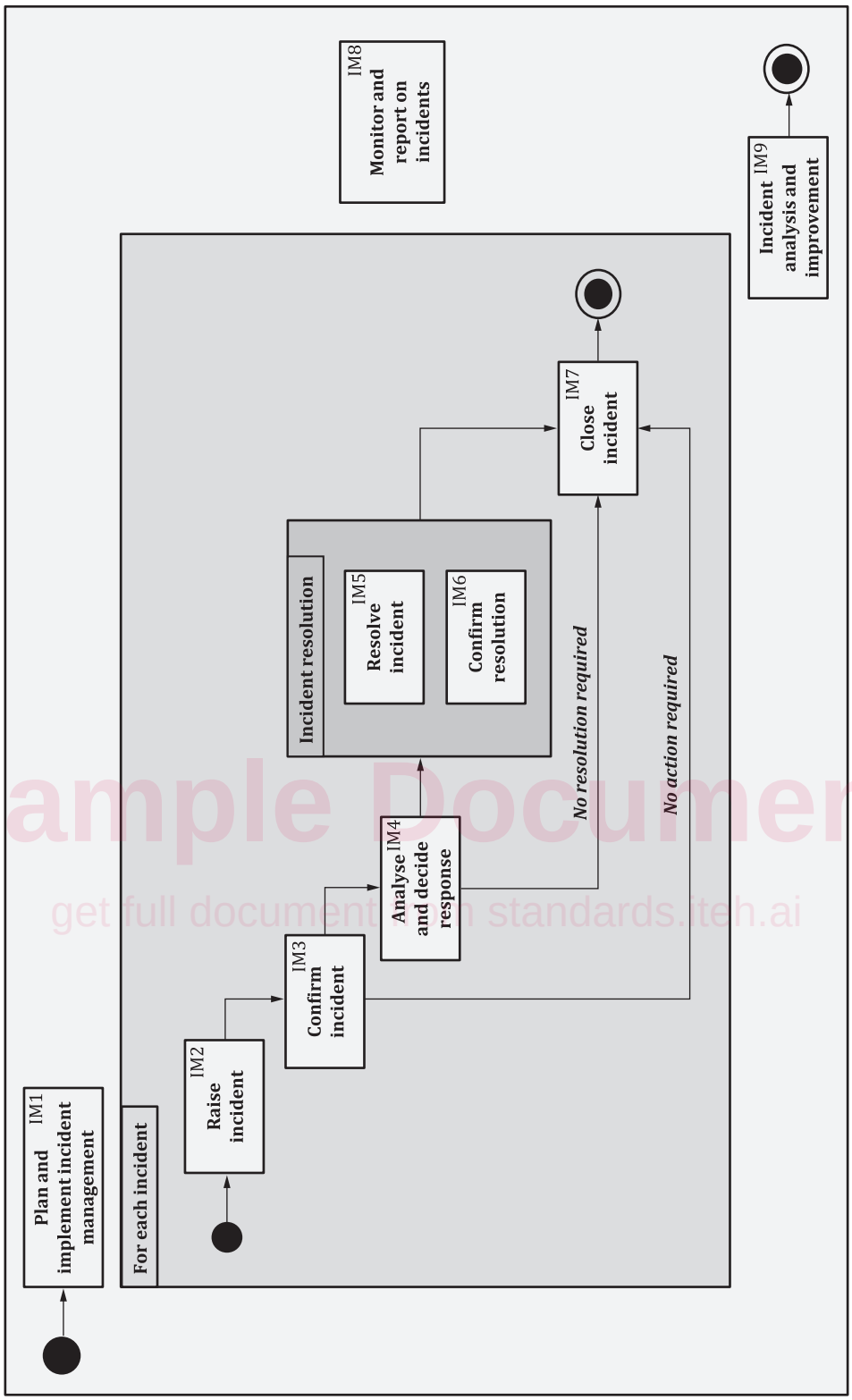
Incident management includes planning how incidents are to be handled by a project or organization (the first activity, IM1, in Figure 1), monitoring and reporting on the status of these incidents (IM8 in Figure 1), and how these incidents are analysed to improve subsequent performance in the project 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 passes 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 can be defined as an organizational practice that can be applied to all projects in an organization. In some situations, this requires the generic plan to be customized for individual projects. Ideally any customization still allows 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 or current incident management processes; and

— current development, verification, validation, test and operational practices.



NOTE 1 Some of the activities in this figure are often combined in practice for smaller projects, organizations or systems.

NOTE 2 Not all possible transitions are shown. Some transitions, notably those that move backwards (e.g. from IM6 to IM5 or IM4), are not shown to increase clarity.

Figure 1 — Incident management process

5.2 Purpose

The purpose of the incident management process is to optimally 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:

a) the incident management plan is agreed;

b) incidents are raised and confirmed;

c) confirmed incidents are analysed and assigned for response;

d) incidents are resolved;

e) incident resolution is monitored;

f) the resolution of incidents is verified, and the incidents are closed;

g) 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 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 and implement incident management (IM1)

This activity consists of the following tasks:

a) The incident management plan shall be established.

b) The incident management plan shall be agreed by the relevant stakeholders.

c) The incident management plan shall be communicated to the relevant stakeholders.

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.

d) 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.

e) The incident management plan shall be implemented.

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 Incident reports can be collected and communicated to the relevant stakeholders using an incident management tool, a test management tool, or on paper.

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, and one is closed.

NOTE 3 If the reported incident appears to be related to a previously raised incident, the two incident reports are usually linked together.

c) If no further action is required:

1) the incident report shall 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 confirm 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 resolution, reporting requirements, and acceptance criteria.

   NOTE In some situations, resolution is not practical, and mitigating actions are more appropriate.

c) If the incident does not require resolution:

   1) the incident report shall 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 or mitigate the incident shall be performed.

   NOTE 1 Sometimes the person or team assigned to perform incident resolution 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 reproduce 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 and caused no unintended regressions elsewhere in the system.

   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 is not 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 have an effect on other artefacts, such as other subsystems or documentation.

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 Confirm resolution (IM6)

This activity consists of the following tasks:

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

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

b) The incident report shall be updated to reflect the resolution result and the target build or version.

c) Resolved incidents shall be progressed to the close incident activity (5.4.8).

d) 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 shall 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 Monitor and report on incidents (IM8)

This activity consists of the following tasks:

a) The timeliness of 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) The collective status of reported incidents shall be determined using relevant metrics (see Annex F).

c) The collective status of reported incidents shall be communicated to relevant stakeholders in the incident management report for the specified reporting period.

5.4.10 Incident analysis and improvement (IM9)

This activity consists of the following tasks:

a) Closed incidents should be analysed to identify root causes and possible improvements.

NOTE 1 In some circumstances, the analysis also includes incidents which have not yet been closed.

NOTE 2 Analysis can identify areas of the system and development process that are problematic, which can be improved in the current or future projects. These areas include:

— the causes of incidents (i.e. problems), which can include technical, managerial, and human factors;

— product weaknesses;

— poor test practices;

— poor incident management practices.

b) Identified improvements should be recorded.

c) Identified improvements should be communicated to the relevant stakeholders for action.

5.5 Information items

As a result of carrying out this process, the following information items shall be produced:

a) incident management plan;

b) incident reports;

c) incident management reports.