Technical Specification

ISO/TS 81001-2-1

First edition
2025-01

Health software and health IT systems safety, effectiveness and security —

Part 2-1: Coordination — Guidance and requirements for the use of assurance cases for safety and security

Sécurité, efficacité et sûreté des logiciels de santé et des systèmes TI de santé —

Partie 2-1: Coordination — Orientations et exigences relatives à l'utilisation des dossiers d'assurance en matière de sûreté et de sécurité

Reference number
ISO/TS 81001-2-1:2025(en)

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

Contents

Page

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).

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 jointly by Technical Committee ISO/TC 215, *Health informatics*, and Technical Committee IEC/TC 62, *Medical equipment, software, and systems*, Subcommittee SC A, *Common aspects of medical equipment, software, and systems*.

A list of all parts in the ISO/IEC 81001 series can be found on the ISO and IEC websites.

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.

Introduction

ISO 81001-1 provides the principles, concepts, terms and definitions for health software and health IT systems, and the key properties of safety, effectiveness and security, across the full life cycle. ISO 81001-1 and all parts of the ISO/IEC 81001 series documents are applicable to stakeholders such as health software manufacturers (including medical device manufacturers) and healthcare delivery organizations (HDOs). This document provides guidance in developing comprehensible and compelling assurance cases in support of safe, secure and effective deployment of health software and health IT systems.

While the benefits of digital health support are widely accepted, the potential for inadvertent and adverse impacts on safety, effectiveness and security caused by health software and health IT systems is also becoming more apparent. Today's sophisticated health software and health IT systems provide advanced levels of decision support and integrate patient data from multiple sources across organizational lines, and across the continuum of care. This creates benefits to the patient and healthcare system, but it also increases the likelihood of software-induced adverse events causing harm to both patients and healthcare organizations. Design flaws, coding errors, security vulnerabilities, incorrect implementation or configuration, data integrity issues, faults in decision support tools, poor alignment with clinical workflows and improper maintenance and use of health software and health IT systems are examples of events with the potential to cause harm. Managing safety, effectiveness and security for health software and health IT systems (including medical devices), requires a comprehensive and coordinated approach to optimizing these three properties.

As health software and health IT systems move through their life cycle stages, multiple organizations are involved. As described in ISO 81001-1, these organizations need to communicate and share information to properly assess and manage the safety, effectiveness, and security in carrying out their respective roles. It is important that this transfer of knowledge and information is sufficiently formalized and predictable so that different stakeholders can communicate and manage these risks in a timely and effective way across life cycle stages and between roles.

Assurance cases are therefore useful tools for communicating risk across the life cycle of health IT systems, given the rigour that is required within, and the inter-dependence of, the different organizations involved at the various life cycle steps. Manufacturers can utilize an assurance case to communicate the risks associated with their products to an HDO. HDOs can build upon the information the manufacturer has provided and develop their assurance case as the product is integrated, configured, and implemented for use within their particular sociotechnical ecosystem context. In this way, assurance cases provide a continuous thread for all roles involved during the life cycle in managing the collective risks of all the components across the health IT infrastructure, including the health software, medical devices and other health IT systems that make up these complex sociotechnical ecosystems. Additionally, assurance case reports can be generated for the purpose of communicating risks from one stakeholder to another as ownership of a health IT systems changes.

IEC 80001-1 provides the roles, responsibilities, and activities necessary for effective risk management to minimize the impact or likelihood of such events and establishes the concept of an assurance case as the principal artefact to demonstrate that the application of risk management has been effective before, during and after the implementation of a health IT system within a health IT infrastructure. The assurance case is the principal mechanism for demonstrating compliance with IEC 80001-1.

Additionally, an assurance case can demonstrate confidence in the safety and security properties of a system throughout its lifecycle and a means for demonstrating the relationship, correlation and improved analysis of safety, security, and effectiveness.

The purpose of this document is to:

— provide guidance to those organisations that are responsible for addressing the requirements of IEC 80001-1 and illustrate how those requirements can be demonstrated through the use of an assurance case;

— provide guidance to illustrate to organisations how the concept of an assurance case can be used to facilitate effective dialogue and management of health software (including medical devices) and health IT system safety and security risks across organisational boundaries and between all stakeholders.

NOTE The 6-step method that is presented in 5.2 is reproduced from original work published in 'The Six-Step Method for Developing Goal Structures' in Reference [9]. The material is reproduced here with the permission of the original author, who retains rights to the material.

Health software and health IT systems safety, effectiveness and security —

Part 2-1: Coordination — Guidance and requirements for the use of assurance cases for safety and security

1 Scope

This document establishes requirements and gives guidance on assurance case framework for healthcare delivery organizations (HDOs) and for health software and medical device manufacturers (MDMs) and can be used to support the communication and information transfer between all parties. An assurance case can be used to communicate information and knowledge about different risks to other roles.

This document establishes:

- an assurance case framework for HDOs and health software and MDMs for identifying, developing, interpreting, updating and maintaining assurance cases.
- one of the possible means to bridge the gap between manufacturers and HDOs in providing adequate information to support the HDOs risk management of IT-networks;
- best practice by leveraging ISO/IEC/IEEE 15026-2 and other standards to identify key considerations and for the structure and contents of an assurance case, e.g. iterative and continuous approaches;
- example structure, method and format to improve the consistency and comparability of assurance cases.

This document is applicable to all parties involved in the health software and health IT systems life cycle, including:

a) organizations, health informatics professionals and clinical leaders specifying, acquiring, designing, developing, integrating, implementing and operating health software and health IT systems, for example health software developers and MDMs, system integrators, system administrators (including cloud and other IT service providers);

b) healthcare service delivery organizations, healthcare providers and others who use health software and health IT systems in providing health services;

c) governments, health system funders, monitoring agencies, professional organizations and customers seeking confidence in an organization's ability to consistently provide safe, effective and secure health software, health IT systems and services;

d) organizations and interested parties seeking to improve communication in managing safety, effectiveness and security risks through a common understanding of the concepts and terminology used in safety, effectiveness and security management;

e) providers of training, assessment or advice in safety, effectiveness and security risk management for health software and health IT systems;

f) developers of related safety, effectiveness and security standards.

This document is for use by organizations and people who build, acquire, operate, maintain, use or decommission health software and health IT systems (including medical devices). It is applicable to all organizations involved, regardless of size, complexity or business model.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security — Part 1: Principles and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 81001-1:2021 and the following 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/

3.1
assumption
intentionally unsubstantiated statement

Note 1 to entry: An assumption is used in the reasoning of a goal.

Note 2 to entry: Adapted from Reference [10].

3.2
assurance
grounds for justified confidence that a goal has been or will be achieved

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.1.1, modified — "claim" was replaced by "goal".]

3.3
argument
connected series of goals intended to establish an overall goal

Note 1 to entry: Adapted from Reference [10].

3.4
confidence
proposition being asserted by the author that is a true or false statement

Note 1 to entry: Adapted from Reference [10].

3.5
goal
true-false statement about the limitations on the values of an unambiguously defined property – called the claim's property – and limitations on the uncertainty of the property's values falling within these limitations during the claim's duration of applicability under stated conditions

Note 1 to entry: Uncertainties may also be associated with the duration of applicability and the stated conditions.

Note 2 to entry: A claim potentially contains the following:

— property of the system-of-interest;

— limitations on the value of the property associated with the claim (e.g. on its range);

— limitations on the uncertainty of the property value meeting its limitations;

— limitations on duration of claim's applicability;

— duration-related uncertainty;

- — limitations on conditions associated with the claim; and
- — condition-related uncertainty.

Note 3 to entry: The term “limitations” is used to fit the many situations that can exist. Values can be a single value or multiple single values, a range of values or multiple ranges of values, and can be multi-dimensional. The boundaries of these limitations are sometimes not sharp, e.g. they can involve probability distributions and can be incremental.

Note 4 to entry: The term ‘claim’ is sometimes used as a synonym for ‘goal’.

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.1.4, modified — The preferred term “claim” was changed to “goal”; Note 4 to entry was added.]

3.6
context
reference to the system documentation towards an assertion regarding capabilities and properties external to the system

Note 1 to entry: A context can be justified by the intended use and notably the intended operational environment of the respective system.

Note 2 to entry: A context can be used in the reasoning of a strategy.

Note 3 to entry: Adapted from Reference [16].

3.7
evidence
directly measurable characteristics of a process and/or product that represent objective, demonstrable proof that a specific activity satisfied a specific requirement

[SOURCE: ISO/IEC 21827:2008, 3.19]

3.8
justification
type of claim which is raised as part of an assurance case and which is not further refined

3.9
solution
reference to an artefact that points to a technical implementation

Note 1 to entry: A solution can be used in the reasoning of a strategy.

3.10
strategy
argument demonstrating plausibility of one (or multiple) goal(s) based on related support in a context, based on assumptions and using evidence, justifications and solutions and other sub goals (which can then not be supported by that strategy instance to ensure cycle-free reasoning)

3.11
responsibility agreement
document(s) that together fully define the responsibilities of all stakeholders

Note 1 to entry: This agreement can be a legal document, e.g. a contract.

[SOURCE: ISO 81001-1:2021, 3.1.9]

3.12
security control
management, operational and technical controls (i.e. safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information

[SOURCE: ISO 12812-1:2017, 3.54]

3.13
security pattern
means of documenting and reusing successful argument structures

Note 1 to entry: Adapted from Reference [15].

4 Assurance case

4.1 Concepts

Assurance that a health IT system achieves certain objectives is particularly important when the system and its interaction with the environment are complex and evolving. Assurance cases establish goal(s) that relate to selected properties of the health IT system and argue for the truth of those goals(s).

Assurance cases are generally developed to support goals in areas such as safety, reliability, maintainability, human factors, operability, and security. Whilst this document focuses on safety and security, assurance case methods are applicable to any property of a system. These assurance cases are often called by more specific names, e.g. safety case or dependability case. ISO/IEC/IEEE 15026-1 provides concepts, terminology, background and a list of standards related to assurance cases.

An assurance case is a structured, solution-based argument used to demonstrate confidence that a system holds a particular critical property.

An argument is a connected, hierarchical series of goals intended to establish an overall goal. The argument in an assurance case shows how a high-level goal is supported by a number of sub goals, which, in turn are supported by detailed presentation of a solution(s). It is the combination of goals and solution that provide confidence in the overall high-level goal made for the characteristic of the system.

A solution which is defined as scientific fact, or empirical outcome, provides a basis that demonstrates that the goal has been achieved. An argument without a solution is unfounded whilst a solution presented out of the context of an argument is unexplained.

Presenting the argument and solution in a structured way reduces the likelihood of uncertainty and allows for a better analysis of the achievement of the set of objectives (the goals).

Additional assurance case concepts such as assumptions, justifications and context enable other factors and considerations to be expressed which will support the interpretation and the validity of the assurance case.

4.2 Healthcare delivery organizations (HDO)

An assurance case can be established for any element of a health IT system, the health IT system itself and the entire health IT infrastructure, addressing any network component, e.g. the radiology network, network communication components, medical devices, accessories and even components of devices.

HDOs can use the assurance case, as outlined in this document, to form part of a broader assurance case addressing additional critical properties such as safety, reliability, maintainability, etc.

HDO's can use this document for one or more of the following:

a) support the understanding and communication of safety and security risks associated with components of the health IT system that are provided by third party organizations;

b) assess and manage safety and security risks associated with the deployment and use of health IT systems and health IT infrastructures in their own organizations;

c) demonstrate their own conformity with IEC 80001-1 and ISO 81001-1.

4.3 Manufacturers

An assurance case is an important tool for providing HDOs with the appropriate level of information about the safety and security characteristics of a manufacturer's product(s) to support the HDOs' risk management of their health IT systems (that can incorporate health software products including medical devices), which are being implemented in the HDOs' health IT infrastructure.

This document also provides guidance to manufacturers in developing a security case to demonstrate confidence in the achievement of IEC/TS 81001-2-2[1].

An assurance case can be treated as a 'living artefact' which begins at the outset of the system/software development lifecycle (SDLC) and is continuously developed and updated during design, production and operation of the manufacturer's product(s).

The assurance case may act as a supporting document to the manufacturer disclosure statement for medical device security (MDS2).

4.4 Other stakeholders

Stakeholders (involved in conformity assessment, certification, regulation, acquisition or audit) can evaluate the assurance case to determine the extent of achievement of the top-level goal (e.g. that the health IT product is safe or secure) and whether this achievement is demonstrated within the allowable uncertainty or risk and any related consequences. The results regarding the top-level goal and its support along with related uncertainties and consequences constitute a basis for rationally managing risk and aiding in decision making.

This document is also for use by organizations who build, acquire, operate, maintain, use or decommission health software and health IT systems (including medical devices), as well as by those creating standards addressing safety, effectiveness and security of health IT systems. It is applicable to all organizations involved, regardless of their size, complexity, or business model.

The quality of artefacts gathered and documented during the development of the assurance case should be agreed to and documented as part of a responsibility agreement between the relevant stakeholders (as currently practised by security assurance cases). This document will provide guidance and methodology, using specific notations, to support, develop and interpret assurance cases in a systematic manner.

4.5 Benefits

The assurance case has been commonly applied to the safety domain, specifically addressing safety concerns for systems, however the use of an assurance case has expanded and nowadays addresses other critical properties such as dependability, reliability, and security across a range of safety critical domains such as automotive, railway, defence and aviation. An assurance case is called a safety case when used to argue the safety of a system. Similarly, they are referred to as assurance cases and dependability cases when arguing respectively.

A significant benefit of an assurance case is that it provides a mechanism to facilitate effective communication of the particular characteristics of a product between stakeholders. The rationale, the justification for the relevance of the rationale and its supporting confirmatory evidence can be presented and appraised in a systematic way.

As a manufacturer, an assurance case can be used to establish confidence that the requirements of a standard have been satisfied. An argument reflecting the architecture of a standard can guide a manufacturer in generating and collating supporting evidence; gaps or weaknesses in the evidence will become apparent.

If a manufacturer incorporates a third-party product in their own product, an assurance case can be used to communicate third party assurance requirements and also to collate and integrate assurance evidence associated with the third party product into the manufacturer's product assurance case.

[1] Under preparation. Stage at the time of publication: IEC/CD TS 81001-2-2.

The concept of an assurance case model or pattern encourages soundness and completeness as it can introduce efficiency and improve the assurance culture within an organization by providing a framework that supports consistency in the assurance process.

The impact of changes or modifications to a product can be more readily assessed if there is an assurance case established for the product. For example, if software changes are proposed to a functional module, the need for and significance of supporting test evidence required to maintain the integrity of that function will be apparent. This contributes to pro-active risk management.

The philosophy of an assurance case provides flexibility to enable the rigour of the assurance case and its supporting evidence base to be proportionate to the risk profile of the product. Justifications or assumptions can be presented to explain why an element of an assurance argument or evidence is not required given the assessed risk profile.

Managing the assurance case as a living artefact provides on-going visibility of assurance maturity and an opportunity to influence its development and final sufficiency. Contradictions in the argument or gaps in the evidence will be revealed sooner in the lifecycle with greater opportunity for correction. The cost of corrective change to a product is proportionate to the phase at which the correction is made, i.e. it is cheaper to correct requirement deficiencies before product design then it is correct them post product implementation.

4.6 Requirements

The following requirements apply when an organization develops an assurance case:

- Goals: The organization shall define one or more goal(s) to express the assurance claim that is being made as part of a new assurance case.
- Justification: The organization shall justify the rationale for the definition of the top-level goal.
- Argument: The organization shall express arguments that logically link the defined goal(s) to the solutions.
- Solutions: The organization shall provide a body of evidence that demonstrates that the goal(s) has been satisfied.

5 General requirements and recommendations

5.1 Principles

The principal objective of an assurance case is to present a well-organised and reasoned proposition, based on objective evidence, that a system is acceptably safe and secure in a given context.

The development of an assurance case is an iterative process and is aligned and integrated within the system development and deployment lifecycle. Formalisation of an assurance case occurs at key lifecycle milestones and supports stakeholder decision making, for example at the point of clinical deployment or system modification.

5.2 Assurance case development process

5.2.1 General

An assurance case can be developed following many different approaches; it is not the purpose of this document to prescribe a specific approach. However, the process for developing safety cases as published in Reference [9] and as incorporated into the [SCSC-141C] Goal Structuring Notation Community Standard[10] has been adopted. This approach, referred to as the “6-step method” is presented in Figure 1 and described in 5.2.2 to 5.2.7.

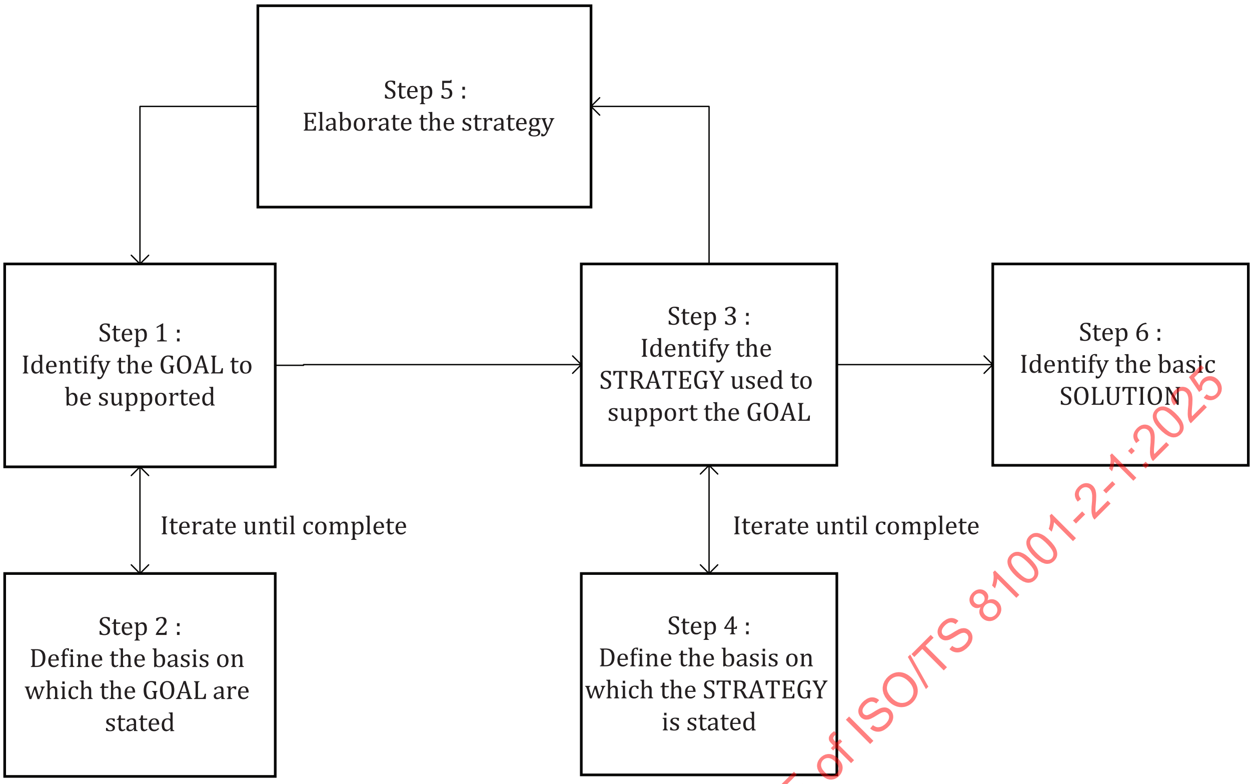
Step 5 :
Elaborate the strategy
Step 1 :
Identify the GOAL to be supported
Step 3 :
Identify the STRATEGY used to support the GOAL
Step 6 :
Identify the basic SOLUTION
Iterate until complete
Iterate until complete
Step 2 :
Define the basis on which the GOAL are stated
Step 4 :
Define the basis on which the STRATEGY is stated

Figure 1 — 6-step method

5.2.2 Step 1: identify the goal

Step 1 establishes the top-level goal of the assurance case that the remainder of the assurance argument supports and substantiates. In establishing the top-goal, the author of the assurance case should consider the intended purpose and recipient of the assurance case and ensure that the top-goal is expressed at an appropriate level of abstraction. For example, the top-goal of an assurance case developed by a medical device manufacturer to support the regulatory compliance of the product could be expressed at a lower level of detail to that of a top-goal associated with demonstrating the safety of health IT infrastructure that includes that product. In the first case, the purpose would relate to satisfying regulatory requirements, and the recipient could be a regulatory body. Assumptions could be declared regarding deployment context but not necessarily argued or evidenced. In the second case, the purpose would relate to organizational deployment of the product as part of a broader health IT infrastructure, and the recipient could be the organization’s top management. There would be less opportunity to make assumptions regarding deployment context; the assurance case would be expected to demonstrate the sufficiency of such.

5.2.3 Step 2: define the basis of the goal

Step 2 establishes the context in which the truth of the goal is to be demonstrated. It is not credible to make a goal that a property holds in all scenarios. The basis of a goal should be clearly and unambiguously explained such that the recipient of the assurance case has sufficient understanding to draw an opinion on the truth of the goal.

Three general themes shall be presented:

- information that defines the system to which the assurance case applies, e.g. technical specification;
- information that defines the environment in which the system is used and how it is used, e.g. care process definition;
- information that supplements the assurance argument, e.g. terms and definitions.

5.2.4 Step 3: identify the strategy

Step 3 establishes the approach through which the goal is substantiated. The strategy should be expressed as a statement that convinces the recipient that the goal it supports is true. Generally, a strategy will decompose a parent-goal into a number of sub goals which in turn are easier to evidence as being true. The strategy should explain the logic which relates the proposition made in the parent-goal with those made in the supporting sub goals.

5.2.5 Step 4: define the basis on which the strategy is stated

Step 4 is similar to Step 2 in that it establishes the context in which the truth of the strategy is to be demonstrated. This can extend to include the rationale as to why the particular strategy was chosen and how it supports the decomposition of the parent-goal into sub goals. Goal structuring notation (GSN) elements of context, assumption and justification can be used to achieve this.

5.2.6 Step 5: elaborate the strategy

Step 5 is essentially a repeat of Steps 1 and is repeated until a solution(s) can be presented that substantiates the related goal. It should be noted that each branch of the assurance argument does not need to be developed to the same level of decomposition.

5.2.7 Step 6: identify the solution

Step 6 identifies evidence that demonstrates that its related goal has been substantiated. A goal can be resolved by one or more solutions, but care is needed to ensure that the understanding of how the solutions support the goal is not lost or confused. Similarly, it is permissible for one solution to substantiate more than one goal, but care is needed to explain the rationale.

The solution should be expressed in sufficient specificity so that it is clear how it supports the goal. For example, referencing a specific test result rather than the overarching test report. Solutions may take the form of a published scientific fact, established state-of-the-art or an empirical outcome regarding a capability or property of the product.

5.3 General considerations

A developed and established assurance case should have the following characteristics.

- Accessible: the assurance case shall be accessible by all stakeholders and as such their needs should be considered. The assurance case should be produced and maintained in a format that doesn't introduce limitations and consideration should be given to the unnecessary inclusion of proprietary information that can introduce restrictions on its circulation.
- Affordable: the cost of developing and producing an assurance case shall be balanced against the benefits of doing so. The risk profile associated with the product can have a bearing on this and influence the breath of the argument and the depth of the evidence.
- Auditable: the assurance case can be influenced by judgements made by personnel that contribute to its development and review. The rationale for and the evidence supporting such judgements should be presented within the scope of the assurance case such that they can be fully understood by other stakeholders. This is also an important consideration in the context of future-proofing an assurance case; updates and amendments may be made by personnel who did not contribute to its original creation.
- Clear: the assurance case shall be comprehensible to its intended recipients and as such consideration should be given to the style in which it is presented. Communicating complex technical arguments can be challenging, but assurance cases shall express all the necessary information as simply and as unambiguously as possible.
- Complete: a principal objective of an assurance case is to demonstrate that all reasonably foreseeable vulnerabilities associated with a product have been identified and that the risk associated with these vulnerabilities has been managed to a level that can be tolerated by the organization that is using the

product. Consequently, the assurance case shall establish confidence that a comprehensive assessment of the risks associated with the product has been completed and present evidence that suitable controls have been implemented and verified. Where there are known gaps or weaknesses, these shall be disclosed and their impact on the assurance case explained.

- Proportionate: care is needed to ensure that the scale of an assurance case remains propionate to the complexity and risk profile associated with the health IT system. To be effective, an assurance case needs to communicate the management of risk as simply and succinctly as possible. Large assurance cases can lead to confusion whilst light assurance cases can reduce confidence. The focus should be on quality rather than quantity.
- Maintained: the assurance case shall be maintained over the lifecycle of the health IT system. If changes are made to the product, its intended use or the environment in which it is used, the impact on of these changes on the assurance case shall be assessed. Changes that impact the argument structure or evidence base should be re-assessed.

5.4 Argument considerations

The assurance argument is expressed through the hierarchical decomposition of the top goal into sub goals to a point where a solution in the form of evidence can be presented to substantiate the validity of the goal.

In order to be able to validate the assurance argument:

- each goal in the assurance case shall be structured and expressed as a predicate statement, i.e. a statement that can be demonstrated to be either true or false (e.g. the sky is blue overhead);
- the set of sub goals at each level of decomposition shall show that the parent goal is achieved;
- the number of levels of decomposition shall be appropriate to the complexity of the safety case or the supporting evidence, or both;
- the rationale for the decomposition of a goal into sub goals should be self-evident or explained by additional text (strategy);
- a counter argument shall not be established at any level of decomposition which could defeat or the parent goal;
- each strand of the argument shall conclude with one or more supporting solutions;
- a distinction shall be made and maintained between product and process-based goals and solutions.

5.5 Evidence considerations

Assurance case evidence (solution) is information, based on fact or expert opinion, which is used to demonstrate the validity of a related assurance case goal.

When selecting evidence:

- the type of solution(s) selected shall demonstrate that the validity of a related goal is appropriate to that goal;
- the solution(s) selected shall demonstrate the validity of the related goal in a clear, conclusive, and objective way;
- the strength of the solution(s) shall be proportionate and appropriate to the degree of risk associated with the related goal;
- the solution shall be preserved and accessible through the life of the assurance case and be reviewed and re-appraised in the context of any changes made to the health IT system.

5.6 Notation

5.6.1 General

Assurance cases can be expressed in a number of different styles including textual, tabular or graphical. In this document, the goal structured notation (GSN)[10] has been adopted.

In its simplest form, GSN uses 6 key elements and 2 relationship types to express the assurance case. These are explained in 5.6.2 to 5.6.9.

5.6.2 Goal

A goal (G) is a proposition, i.e. a true-false statement that demonstrates the validity of the assurance case. A goal can be supported by one or more sub goals. The architecture of goals and the relationship between them establishes the assurance argument.

A goal (Figure 2) is depicted as a rectangle with a {goal identifier} and <goal statement>. The identifier is unique.

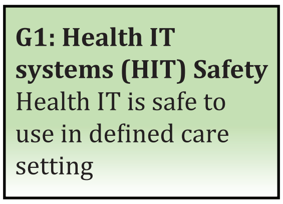
G1: Health IT systems (HIT) Safety
Health IT is safe to use in defined care setting

Figure 2 — Goal

5.6.3 Strategy

The strategy describes the nature of the reasoning that exists between a goal and its supporting sub goal(s). The strategy shall explain to the reader how the sub goals support the parent goal. If this relationship is simple and apparent, then a goal can be described directly without the use of a strategy. A parent goal may be supported by more than one strategy.

A strategy (Figure 3) is depicted as a parallelogram with a {strategy identifier} and <strategy statement>. The identifier is unique.

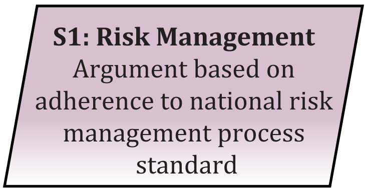
S1: Risk Management
Argument based on adherence to national risk management process standard

Figure 3 — Strategy

5.6.4 Solution

The assurance case argument is developed to a level of detail where a solution(s) can be presented that supports the truth of the related goal. For an assurance case to be complete and compelling, all the lowest level goals are supported by one or more solutions.

A solution (Figure 4) is depicted as a circle with a {solution identifier} and <solution statement>. The identifier is unique.

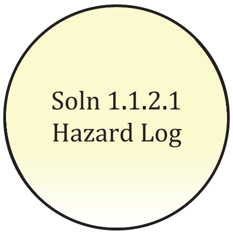

Figure 4 — Solution

5.6.5 Context

A goal can only be asserted to be true in a defined context. The context element is used to include additional information that supports the validity of a goal. An example of context can be a definition of the intended use of the health IT (HIT) system: if the HIT system is used in a different way, then it is possible that the assurance case does not hold. The context will apply to all elements that support the goal, so care is needed not to introduce an element to the assurance case that invalidates or contradicts it.

A context may also be applied to a strategy in order to provide supplementary information or to define terms that may be used in defining the strategy.

A context (Figure 5) is depicted as a stadium with a {context identifier} and <context statement>. The identifier is unique.

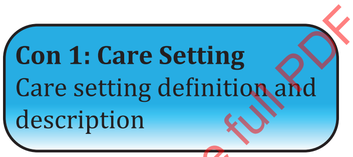

Figure 5 — Context

5.6.6 Assumption

An assumption is an intentionally, unsubstantiated statement that relates to a given goal. The assumption applies to all elements that support the goal that the assumption is associated with.

An assumption (Figure 6) is depicted as an oval with an A at the top-right or bottom-right, an {assumption identifier} and <assumption statement>. The identifier is unique.

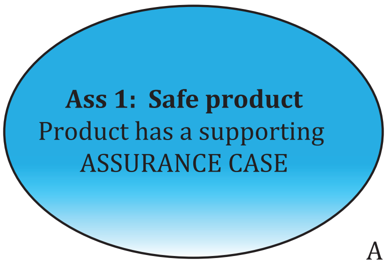

Figure 6 — Assumption

5.6.7 Justification

A justification is used to provide the rationale of including an element within an assurance case and as such can relate to a goal or strategy. Unlike other elements, a justification only applies to the element to which it is connected.

A justification (Figure 7) is depicted as an oval with a J at the top-right or bottom-right, a {justification identifier} and <justification statement>. The identifier is unique.

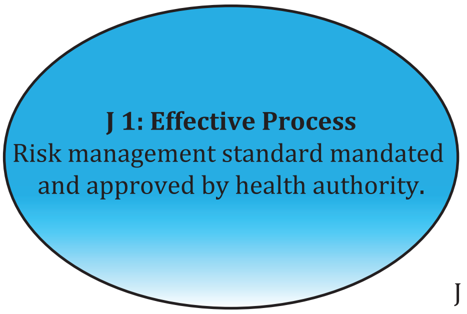
J 1: Effective Process
Risk management standard mandated and approved by health authority.
J

Figure 7 — Justification

5.6.8 SupportedBy relationship

A SupportedBy relationship is used to explain the relationship between elements within the assurance case.

It is depicted (Figure 8) as a line with a solid arrowhead. Permitted SupportedBy relationships are: goal-to-goal, goal-to-strategy, goal-to-solution, strategy-to-goal.

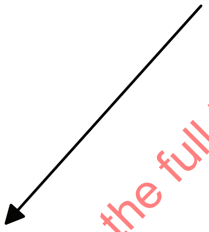

Figure 8 — SupportedBy

5.6.9 InContextOf relationship

An InContextOf relationship is used to explain the relationship between elements in an assurance case and additional narrative that has a bearing on that element.

It is depicted (Figure 9) as a line with a hollow arrowhead. Permitted InContextOf relationships are: goal-to-context, goal-to-assumption, goal-to-justification, strategy-to-context, strategy-to-assumption and strategy-to-justification.

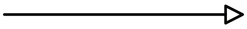

Figure 9 — InContextOf

6 Developing an assurance case using GSN

6.1 General

Clause 6 illustrates the development of an assurance case using GSN notation. The GSN model is derived from the one established by Habli et al.[11] The 6-step method described in Clause 5 is followed.

6.2 Step 1: identify the goal

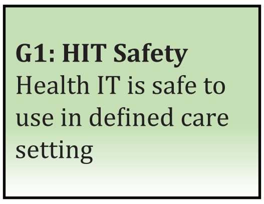

Figure 10 — Top goal

In Figure 10, the top goal, G1, is that the IT system is safe to use in the defined care setting. Further elaboration is needed to establish the context in which this goal is stated or expressed.

6.3 Step 2: define the basis on which the goal is stated

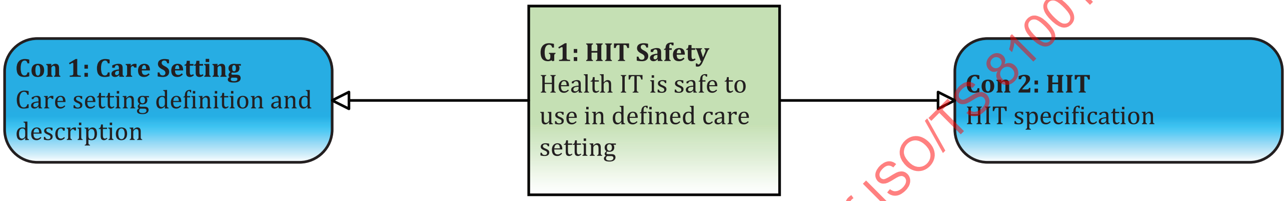
Con 1: Care Setting
Care setting definition and description
G1: HIT Safety
Health IT is safe to use in defined care setting
Con 2: HIT
HIT specification

Figure 11 — Context

In Figure 11, context Con 1 and Con 2 are introduced to provide a definition of the care setting in which the HIT system should be used and a definition of the HIT system itself. In practice, this would be established through project documentation.

6.4 Step 3: identify the strategy used to support the goal

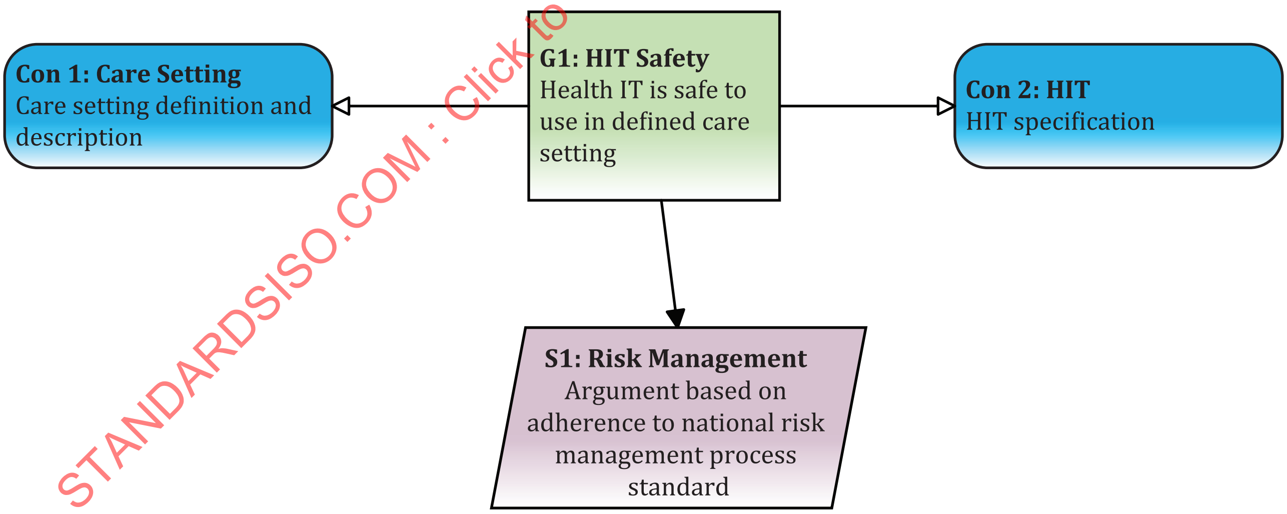
Con 1: Care Setting
Care setting definition and description
G1: HIT Safety
Health IT is safe to use in defined care setting
Con 2: HIT
HIT specification
S1: Risk Management
Argument based on adherence to national risk management process standard

Figure 12 — Strategy

In Figure 12, strategy S1 establishes that safe use of the HIT system in the defined care setting will be achieved by following a risk management process, in this case one specified and approved by the national health authority.

6.5 Step 4: define the basis on which the strategy is stated

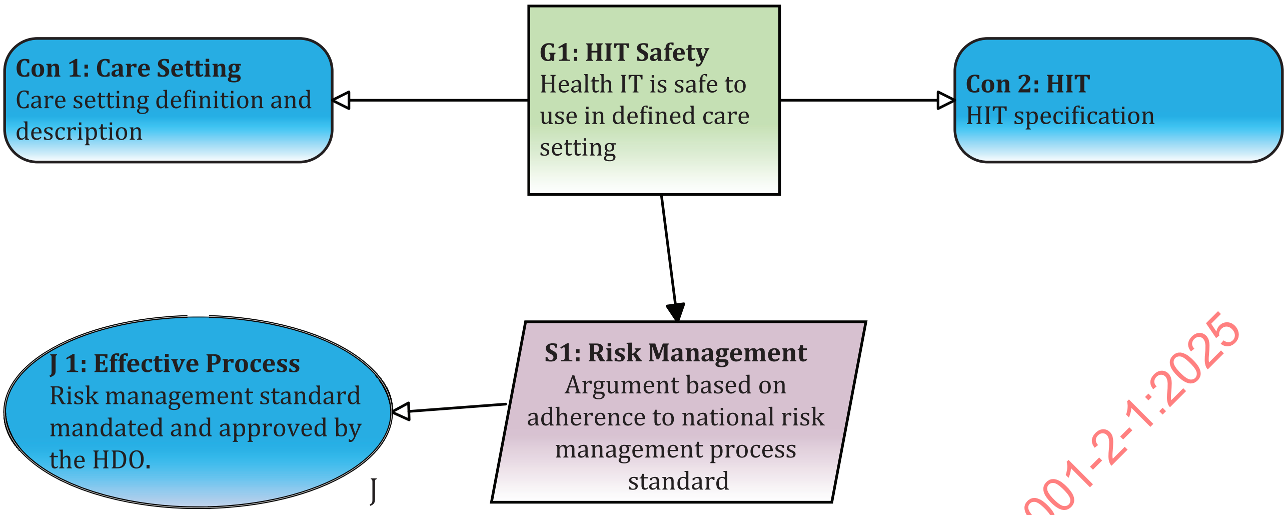
Con 1: Care Setting
Care setting definition and description
G1: HIT Safety
Health IT is safe to use in defined care setting
Con 2: HIT
HIT specification
J 1: Effective Process
Risk management standard mandated and approved by the HDO.
J
S1: Risk Management
Argument based on adherence to national risk management process standard

Figure 13 — Justification

In Figure 13, justification J1 provides the rationale for conforming with a risk management standard. The standard establishes a risk management framework that the national health authority considers appropriate when deploying and using HIT systems.

6.6 Step 5: elaborate the strategy

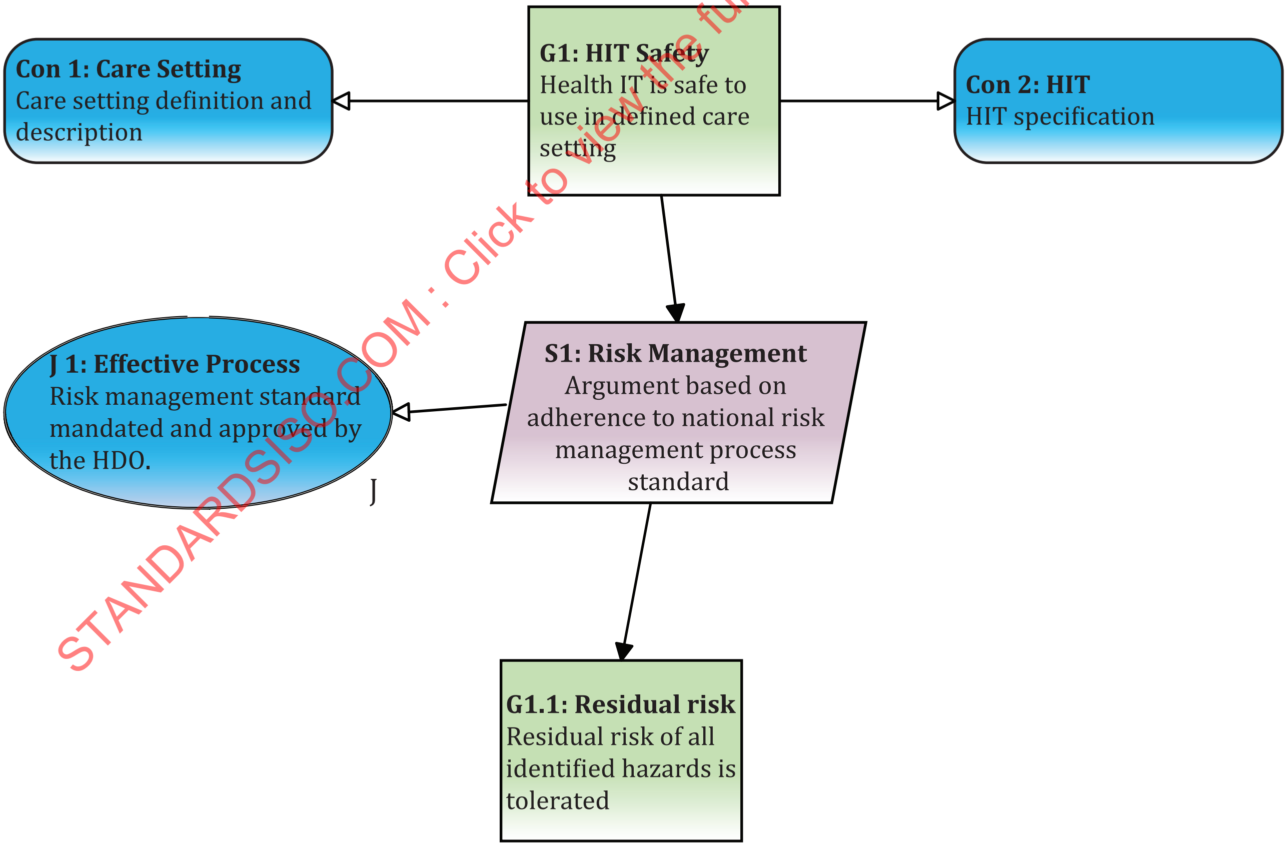
Con 1: Care Setting
Care setting definition and description
G1: HIT Safety
Health IT is safe to use in defined care setting
Con 2: HIT
HIT specification
J 1: Effective Process
Risk management standard mandated and approved by the HDO.
J
S1: Risk Management
Argument based on adherence to national risk management process standard
G1.1: Residual risk
Residual risk of all identified hazards is tolerated

Figure 14 — Sub goal

In Figure 14, G1.1, establishes that, by following a standard national process, the organization can demonstrate that the residual risk of all identified hazards has been reduced to a level that can be tolerated by the organization. Further elaboration is needed to explain key concepts regarding this goal.

6.7 Repeat Step 2: define the basis on which the goal is stated

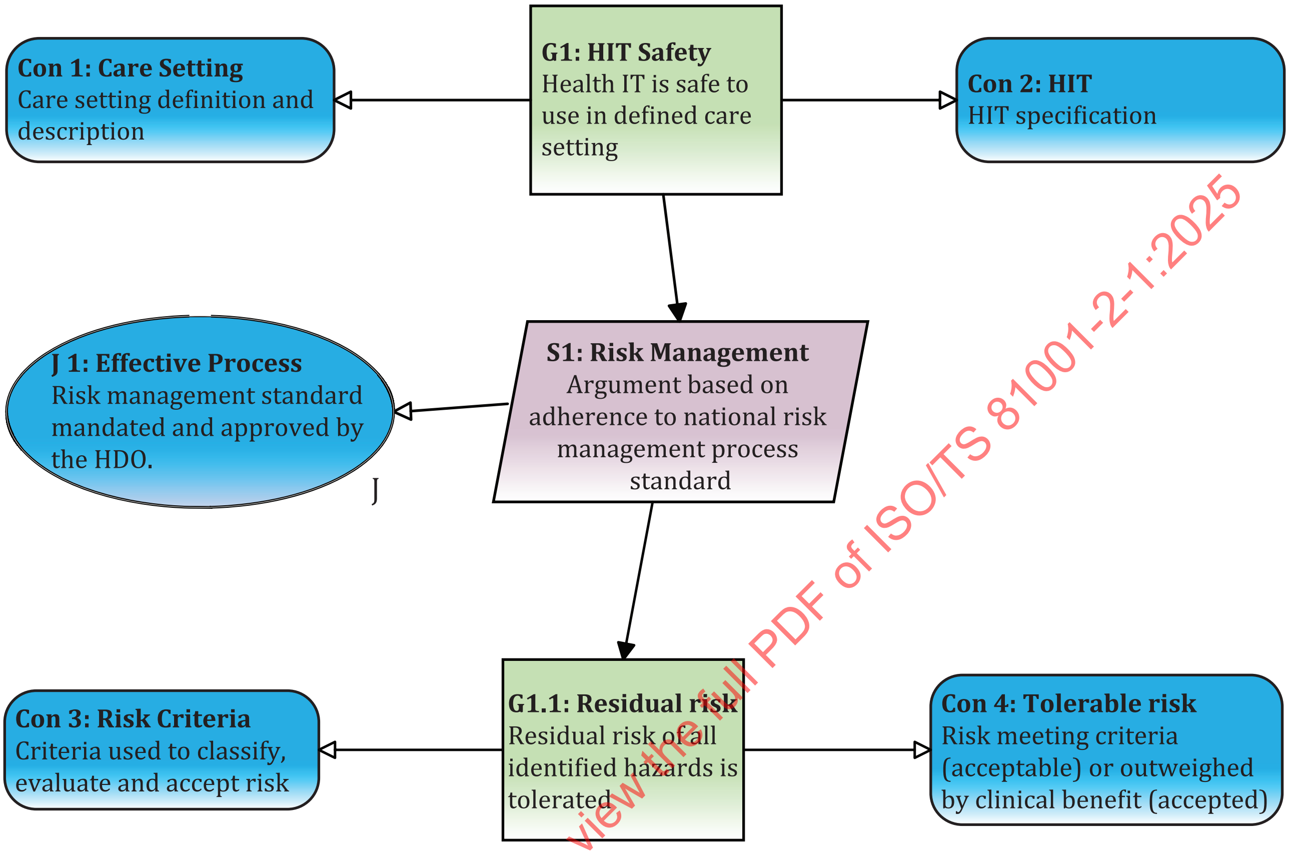
Con 1: Care Setting
Care setting definition and description
G1: HIT Safety
Health IT is safe to use in defined care setting
Con 2: HIT
HIT specification
J 1: Effective Process
Risk management standard mandated and approved by the HDO.
J
S1: Risk Management
Argument based on adherence to national risk management process standard
Con 3: Risk Criteria
Criteria used to classify, evaluate and accept risk
G1.1: Residual risk
Residual risk of all identified hazards is tolerated
Con 4: Tolerable risk
Risk meeting criteria (acceptable) or outweighed by clinical benefit (accepted)

Figure 15 — Context for sub goal

In Figure 15, context Con 3 is introduced to provide a definition of the criteria that is used to estimate, evaluate and accept risk within the organization. Context 4 establishes the concept of tolerable risk within the organisation. Risk can be tolerated if it meets the defined criteria (acceptable) or if a clinical benefit can be demonstrated (accepted).

6.8 Repeat Step 4: define the basis on which the strategy is stated

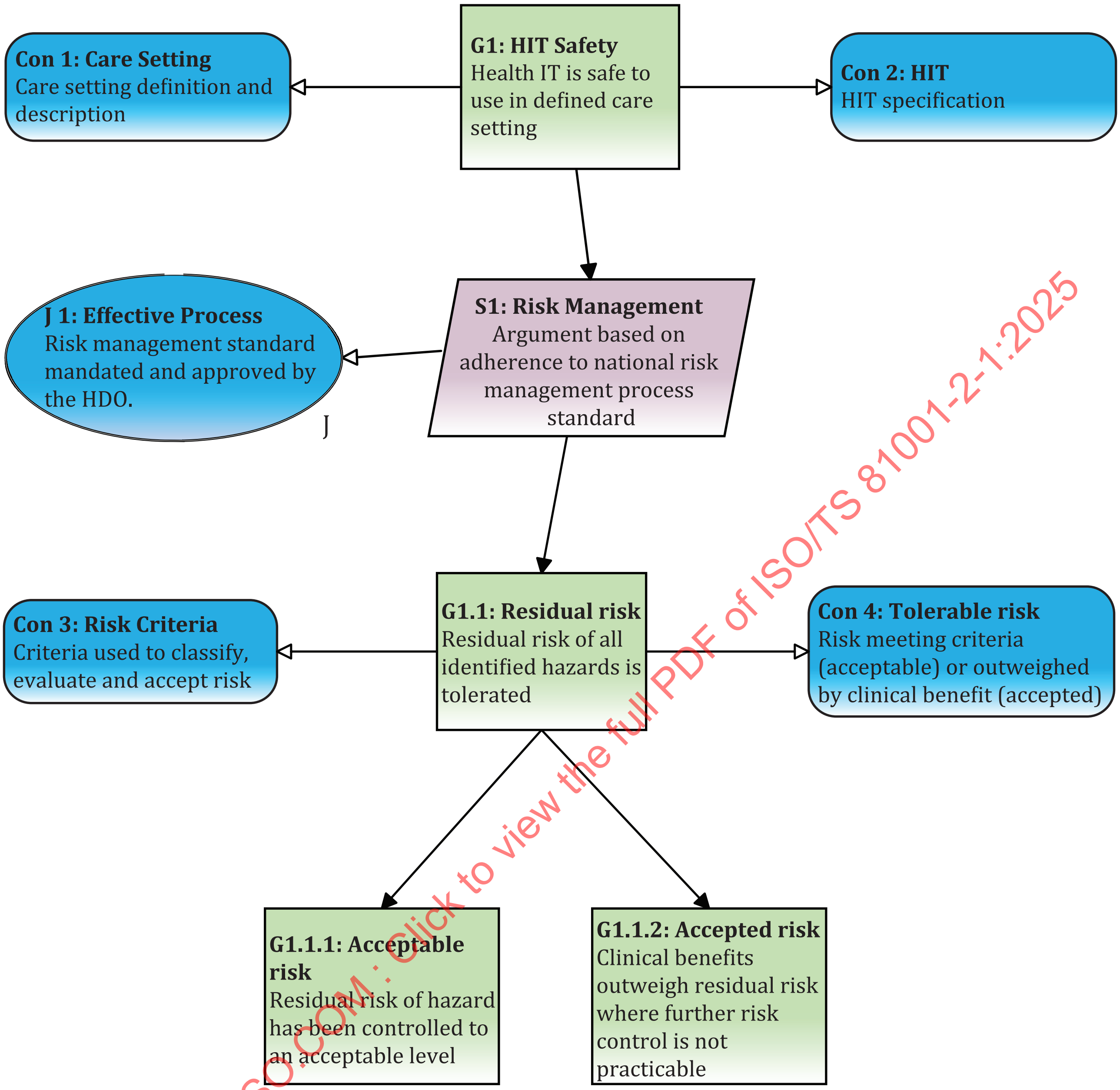
G1: HIT Safety
Health IT is safe to use in defined care setting
Con 1: Care Setting
Care setting definition and description
Con 2: HIT
HIT specification
J 1: Effective Process
Risk management standard mandated and approved by the HDO.
J
S1: Risk Management
Argument based on adherence to national risk management process standard
Con 3: Risk Criteria
Criteria used to classify, evaluate and accept risk
G1.1: Residual risk
Residual risk of all identified hazards is tolerated
Con 4: Tolerable risk
Risk meeting criteria (acceptable) or outweighed by clinical benefit (accepted)
G1.1.1: Acceptable risk
Residual risk of hazard has been controlled to an acceptable level
G1.1.2: Accepted risk
Clinical benefits outweigh residual risk where further risk control is not practicable

Figure 16 — Elaboration of sub goal

In Figure 16, goal G1.1 can be elaborated directly through sub goals G1.1.1 and G1.1.2 which collectively establish that the risk of each hazard identified through the application of the national risk management process is either acceptable or can be accepted, as a clinical benefit can be demonstrated which outweighs the residual risk.

6.9 Step 6: identify the basic solution

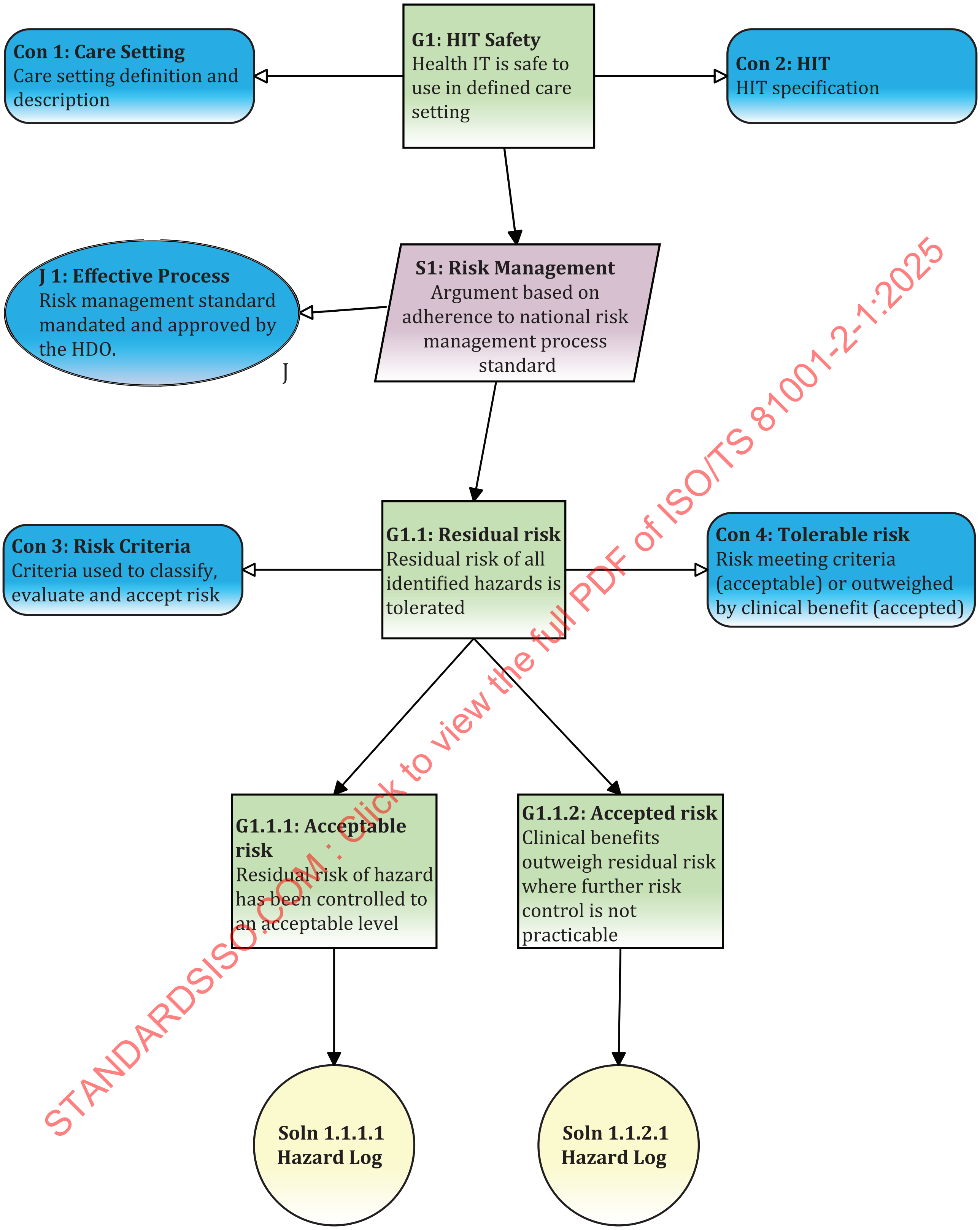
Con 1: Care Setting
Care setting definition and description
G1: HIT Safety
Health IT is safe to use in defined care setting
Con 2: HIT
HIT specification
J 1: Effective Process
Risk management standard mandated and approved by the HDO.
J
S1: Risk Management
Argument based on adherence to national risk management process standard
Con 3: Risk Criteria
Criteria used to classify, evaluate and accept risk
G1.1: Residual risk
Residual risk of all identified hazards is tolerated
Con 4: Tolerable risk
Risk meeting criteria (acceptable) or outweighed by clinical benefit (accepted)
G1.1.1: Acceptable risk
Residual risk of hazard has been controlled to an acceptable level
G1.1.2: Accepted risk
Clinical benefits outweigh residual risk where further risk control is not practicable
Soln 1.1.1.1
Hazard Log
Soln 1.1.2.1
Hazard Log

Figure 17 — Solutions

In Figure 17, solutions Soln 1.1.1.1 and Soln 1.1.2.1 provide the evidence that the two respective goals have been achieved. In practice, the Hazard Logs will provide an index to specific evidence artefacts that substantiate the goal for each identified hazard. This could include design and test evidence demonstrating the effective implementation of a system design feature or a benefits-risk analysis report to support the deployment of the HIT system.

The use of GSN and the application of the “6-step method” is illustrated in example assurance case models presented in Annexes A, B and C.

- Annex A presents a high-level assurance case model that reflects that the HDO has adopted IEC 80001-1:2021 to manage the risk associated with its HIT system implementation.
- Annex B presents a detailed assurance case model that illustrates how the specific requirements of IEC 80001-1:2021 are addressed. This assurance case model can be used to support a conformity assessment against IEC 80001-1:2021.
- Annex C presents a detailed assurance case model that illustrates how the safety characteristics of an AI based product can be assured from a perspective of product development and use.

The use of natural language to express an assurance case is illustrated in example assurance case models presented in Annex D:

- Annex D presents a natural language representation of the high-level GSN assurance case model presented in Annex A that reflects that the HDD has adopted ISO 80001:2021 to manage the risk associated with its HIT system implementation.

7 Assurance case change management

An assurance case can be managed as a live artefact and kept up to date, reflecting the current state of assurance. For the purposes of traceability, change management procedures should be applied when an assurance case is updated.

Examples of when an assurance case can be revised include the following non-exhaustive scenarios:

a) when the supporting information used to inform the development of the assurance case changes, e.g. changes are made to the intended use of a medical device, the operational environment or interfaces;

b) when an incident occurs, which requires reporting and/or mitigation;

c) when a medical device is added to a health IT network;

d) when a medical device is removed from a health IT network;

e) when additional safety or security controls, or both, are required to further protect against identified risk;

f) when there is a need to communicate between organisations (e.g. new functionality, change in intended use case).

8 Security assurance case

A security assurance case complements the security risk management process. The objectives are:

- to reduce the time required to develop the assurance case by providing a repeatable and systematic step-by-step process;
- to reduce the complexity often associated with the development of assurance cases;
- to provide a visible traceability matrix linking the assurance case to security threats and vulnerabilities identified during risk management;
- to reduce the likelihood of missing a step in the argument;
- to improve the readability of the assurance case;

- to provide confidence regarding the integrity of the evidence collected based on the information presented in the argument.

The process of developing the security assurance case is not intended to replace a risk management process nor does it generate new processes, rather, the security assurance case should complement the risk management process with a reference to, or inclusion of, the following supporting documentation by manufacturers and HDOs:

- information regarding the intended use of the medical device, operational environment, network structure, interfaces, boundaries etc.;
- information regarding system description, security objectives and assets to be protected;
- justification for the selection of security capabilities;
- justification for the non-selection of security capabilities;
- assets being protected by specific security capability;
- risk acceptability criteria policy;
- all identified unacceptable threats or vulnerabilities;
- threat, vulnerability or risk log;
- impact, threat scenario or consequence information;
- reference to source for selection of security controls.

The above information becomes part of and remains with the security assurance case from concept phase through to development, operation, and retirement. Supporting information such as this can aid in better design choices, better maintenance during operation and more efficient and informative feedback practices.

Clause 8 is not intended to provide exhaustive guidance for the application of a risk management process, nor does it mandate the use of any particular risk management process, however IEC 80001-1 provides guidance on how to carry out risk management for medical IT networks. Similarly, ISO 14971 provides guidance for the process of conducting risk management for medical devices. For risk management processes such as risk/benefit analysis, which is not covered in this document, HDOs and manufacturers refer to IEC 80001-1, and manufacturers refer to ISO 14971.

IEC 80001-1:2021, Annex C provides additional guidance on the use of assurance cases for knowledge transfer. The manufacturer security pattern (IEC 80001-1:2021, Figure C.3) provides the recommended structure and focus on threat and vulnerability related to security risks. The HDO safety and security patterns (IEC 80001-1:2021, Figure C.4 and C.5) demonstrate the interdependency and appropriate level of information provided between manufacturer and HDO.

Annex E provides assurance case notation cross reference and comparison of terminology used across different assurance case notations.

Annex F provides a summary of assurance case requirements relative to organizations.

Annex A
(informative)

Generic risk-based HIT assurance case pattern

Figure A.1 presents a generic risk-based assurance case, expressed using GSN. Table A.1 explains the contribution of each assurance component in achieving the assurance case.

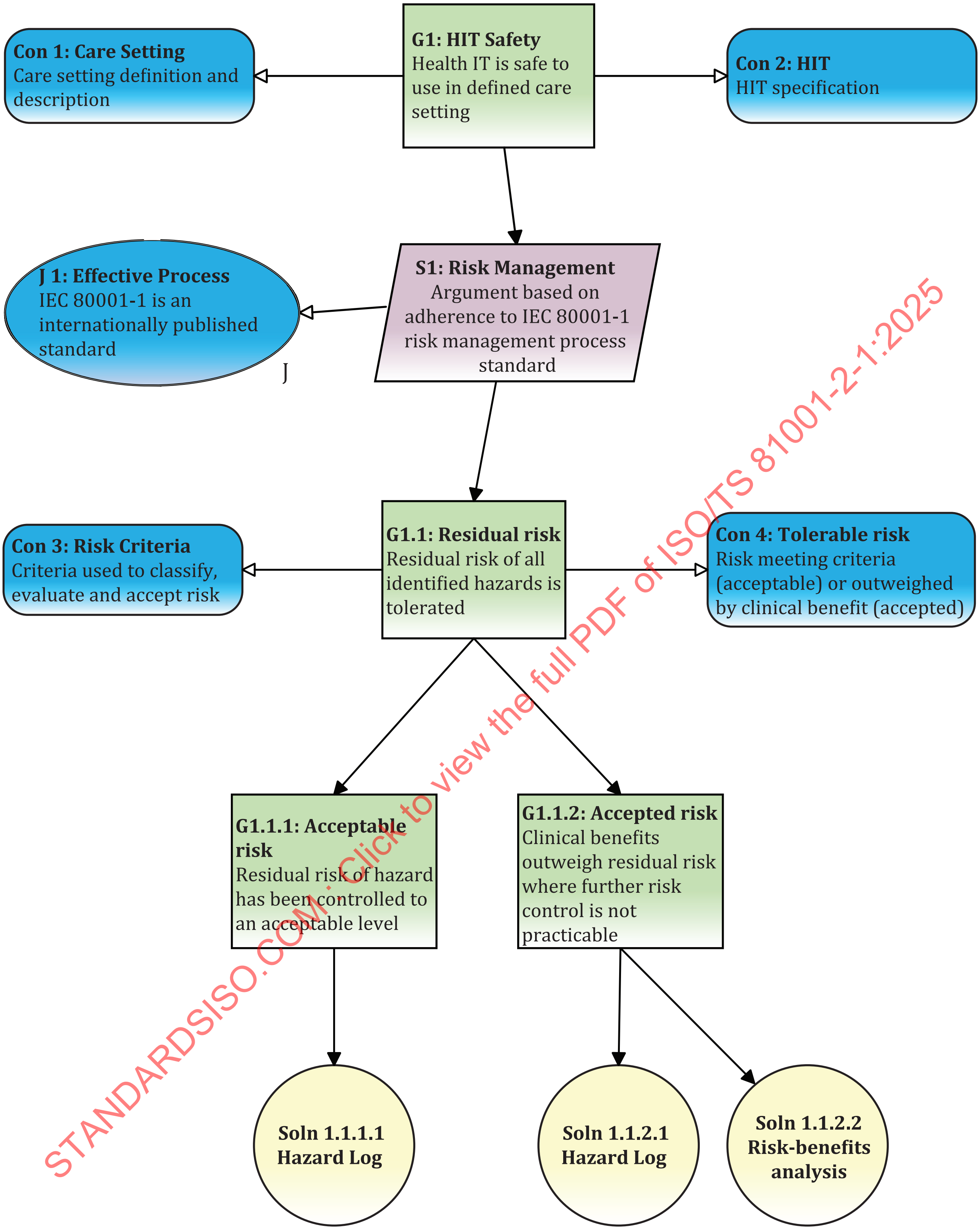
Con 1: Care Setting
Care setting definition and description
G1: HIT Safety
Health IT is safe to use in defined care setting
Con 2: HIT
HIT specification
J 1: Effective Process
IEC 80001-1 is an internationally published standard
J
S1: Risk Management
Argument based on adherence to IEC 80001-1 risk management process standard
Con 3: Risk Criteria
Criteria used to classify, evaluate and accept risk
G1.1: Residual risk
Residual risk of all identified hazards is tolerated
Con 4: Tolerable risk
Risk meeting criteria (acceptable) or outweighed by clinical benefit (accepted)
G1.1.1: Acceptable risk
Residual risk of hazard has been controlled to an acceptable level
G1.1.2: Accepted risk
Clinical benefits outweigh residual risk where further risk control is not practicable
Soln 1.1.1.1
Hazard Log
Soln 1.1.2.1
Hazard Log
Soln 1.1.2.2
Risk-benefits analysis

Figure A.1 — Generic risk-based Health IT (HIT) assurance case pattern

Table A.1 — Health IT (HIT) assurance case narrative

Assurance case component	Explanation
G1	Establishes a top-level claim that the HIT system is safe to use in the defined care setting. This claim is established in the context of (Con 1) which defines the care setting in which the HIT system is to be used and (Con 2) which defines the HIT system itself.
S1	Defines the way in which G1 will be achieved, i.e. by the HDO implementing and following a risk management process that is conformant with IEC 80001-1. This is justified (J1) in the context of IEC 80001-1 being an internationally published risk management standard.
G1.1	Establishes a claim that the residual risk of all identified hazards has been managed to a level that can be tolerated by the HDO. This is claimed in the context (Con 3) of the risk criteria used by the HDO and that the residual risk level meets the tolerability criteria (Con 4) established by the HDO. Con 4 establishes that tolerability is defined as either that the risk meets an acceptable threshold or that the risk is accepted in circumstances of unacceptable risk because clinical benefit is to be gained through the HIT system deployment.
G1.1.1	Establishes a claim that the residual risk of an identified hazard is acceptable. This is demonstrated through reference to the hazard log (Soln 1.1.1.1) which summarises and evidences the risk management activities related to the hazard.
G1.1.2	Establishes a claim that the residual risk of an identified hazard is accepted. This is demonstrated through reference to the hazard log (Soln 1.1.2.1) which summarises and evidences the risk management activities related to the hazard. It will also be supported by a benefits-risk analysis (Soln 1.1.2.2).

Annex B
(informative)

IEC 80001-1 Compliance assurance case pattern

Figures B.1 to B.8 illustrates how the requirements of IEC 80001-1:2021 can be depicted as an assurance case, using GSN. Elements of the assurance case indicate where specific requirements of IEC 80001-1:2021 are addressed.

Figure B.1 establishes the overarching goal that the health IT system is acceptably safe and secure for intended use by the health delivery organization. It defines the context in which this is claimed and that this is achieved through conformance with IEC 80001-1:2021.

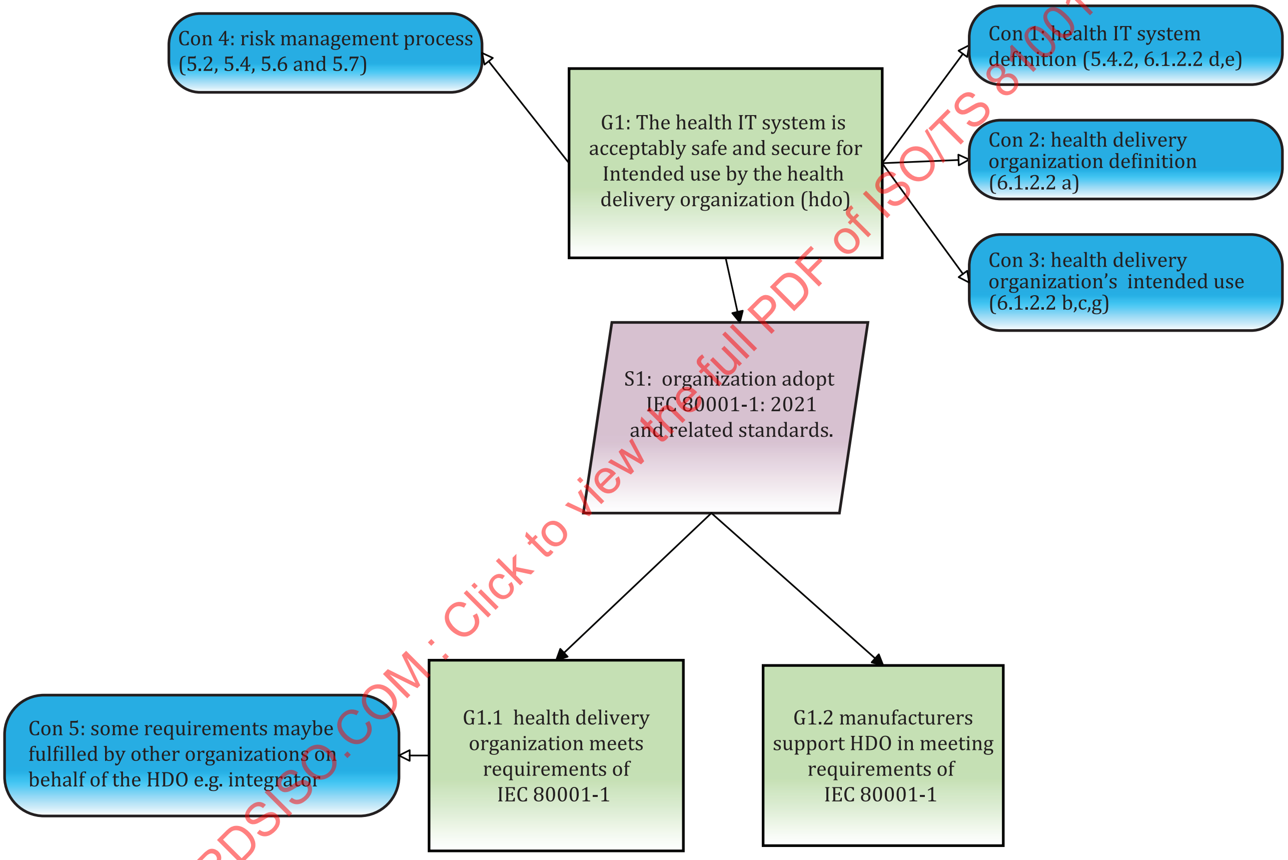
Con 4: risk management process (5.2, 5.4, 5.6 and 5.7)
G1: The health IT system is acceptably safe and secure for Intended use by the health delivery organization (hdo)
Con 1: health IT system definition (5.4.2, 6.1.2.2 d,e)
Con 2: health delivery organization definition (6.1.2.2 a)
Con 3: health delivery organization's intended use (6.1.2.2 b,c,g)
S1: organization adopt IEC 80001-1: 2021 and related standards.
Con 5: some requirements maybe fulfilled by other organizations on behalf of the HDO e.g. integrator
G1.1 health delivery organization meets requirements of IEC 80001-1
G1.2 manufacturers support HDO in meeting requirements of IEC 80001-1

Figure B.1 — Goal G1

Figure B.2 establishes a sub goal that the HDO meets the requirements of IEC 80001-1:2021 with regard to safety and security risk characteristics.

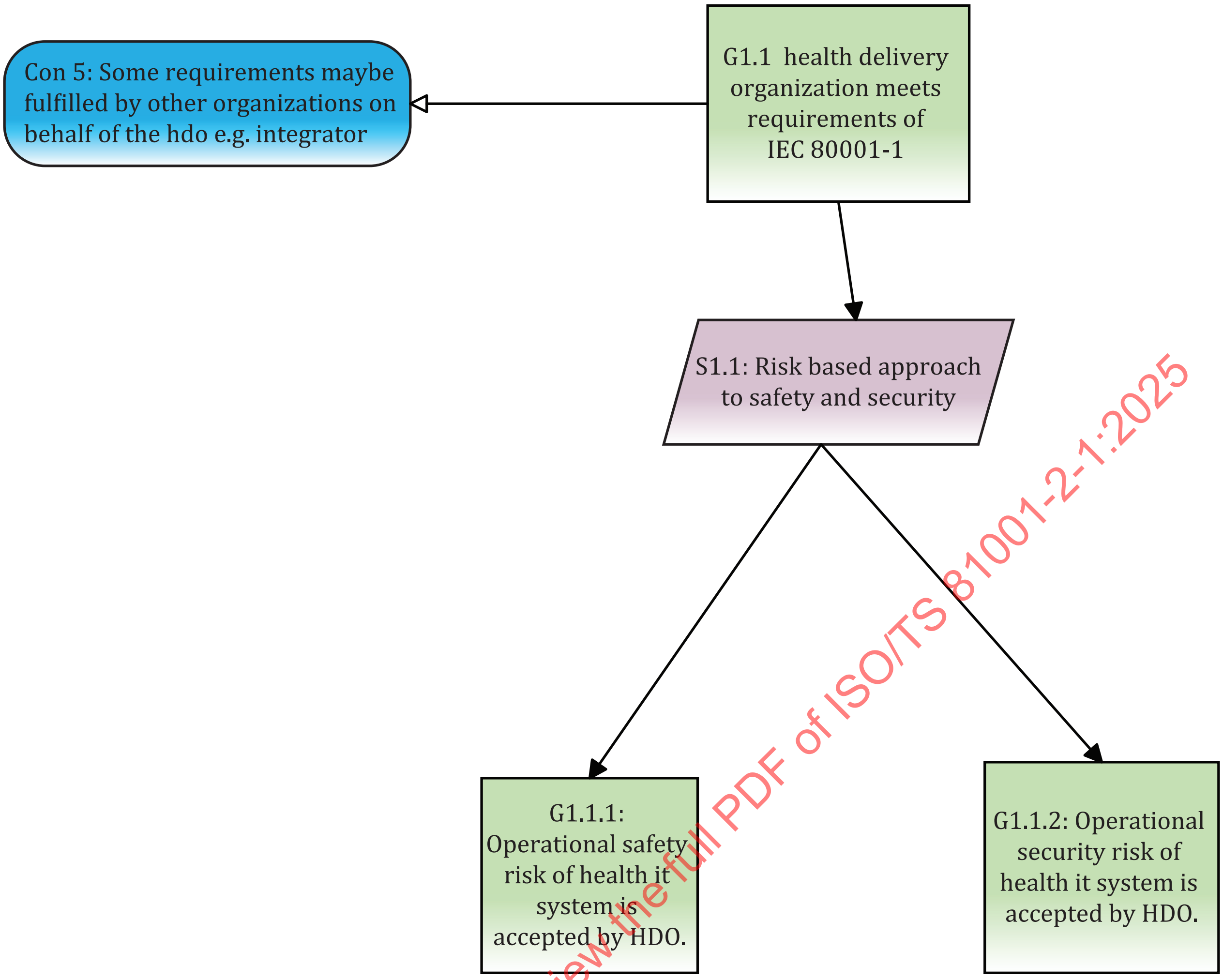
Con 5: Some requirements maybe fulfilled by other organizations on behalf of the hdo e.g. integrator
G1.1 health delivery organization meets requirements of IEC 80001-1
S1.1: Risk based approach to safety and security
G1.1.1: Operational safety risk of health it system is accepted by HDO.
G1.1.2: Operational security risk of health it system is accepted by HDO.

Figure B.2 — Goal G1.1

Figure B.3 supports Figure B.2 and establishes a sub goal that the operational safety risk of the HIT system is accepted by the HDO’s top management.

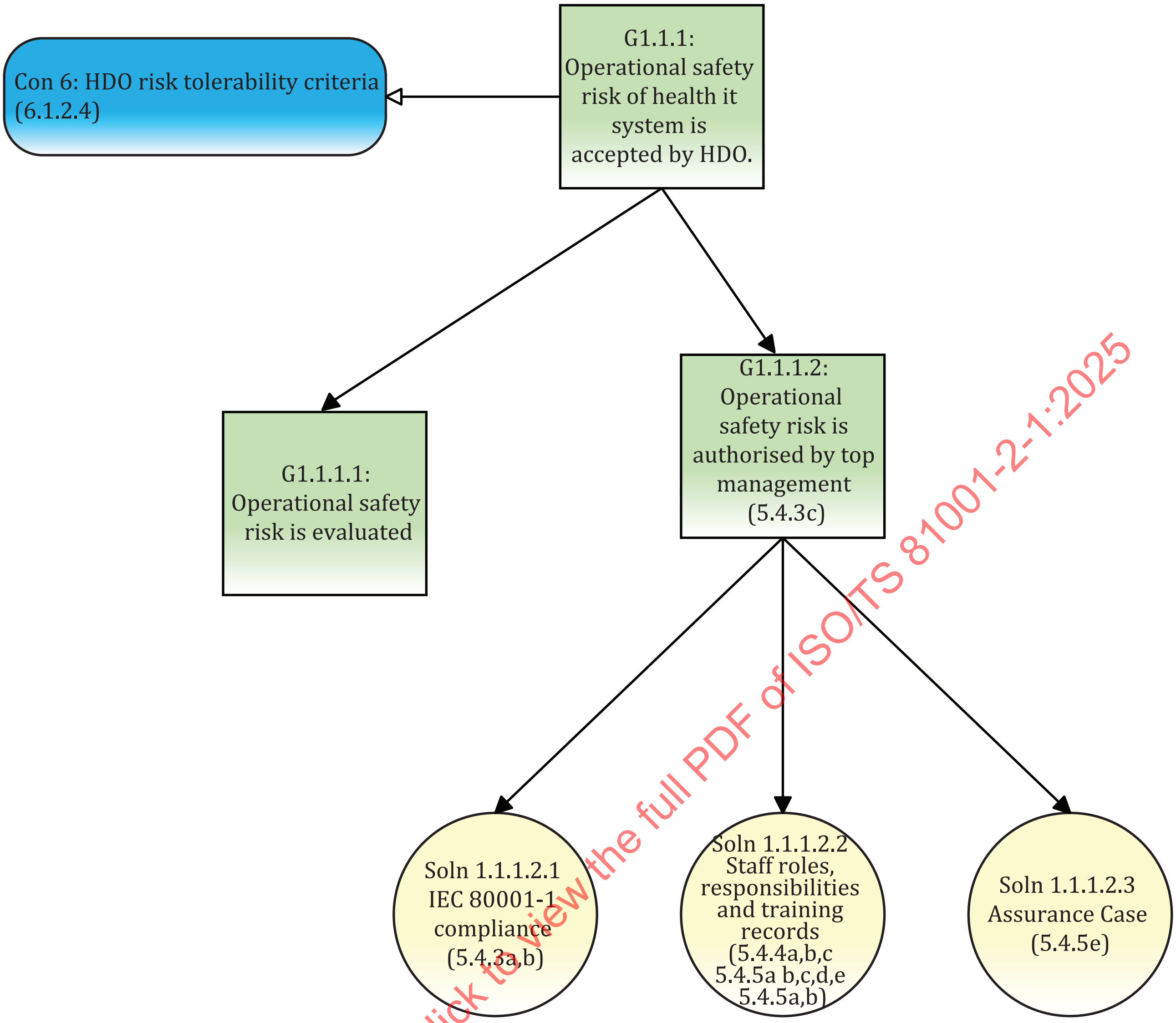
Con 6: HDO risk tolerability criteria (6.1.2.4)
G1.1.1: Operational safety risk of health it system is accepted by HDO.
G1.1.1.1: Operational safety risk is evaluated
G1.1.1.2: Operational safety risk is authorised by top management (5.4.3c)
Soln 1.1.1.2.1 IEC 80001-1 compliance (5.4.3a,b)
Soln 1.1.1.2.2 Staff roles, responsibilities and training records (5.4.4a,b,c 5.4.5a b,c,d,e 5.4.5a,b)
Soln 1.1.1.2.3 Assurance Case (5.4.5e)

Figure B.3 — Goal G1.1.1

Figure B.4 supports Figure B.3 and establishes a sub goal that the operational safety risk of the HIT system has been evaluated.

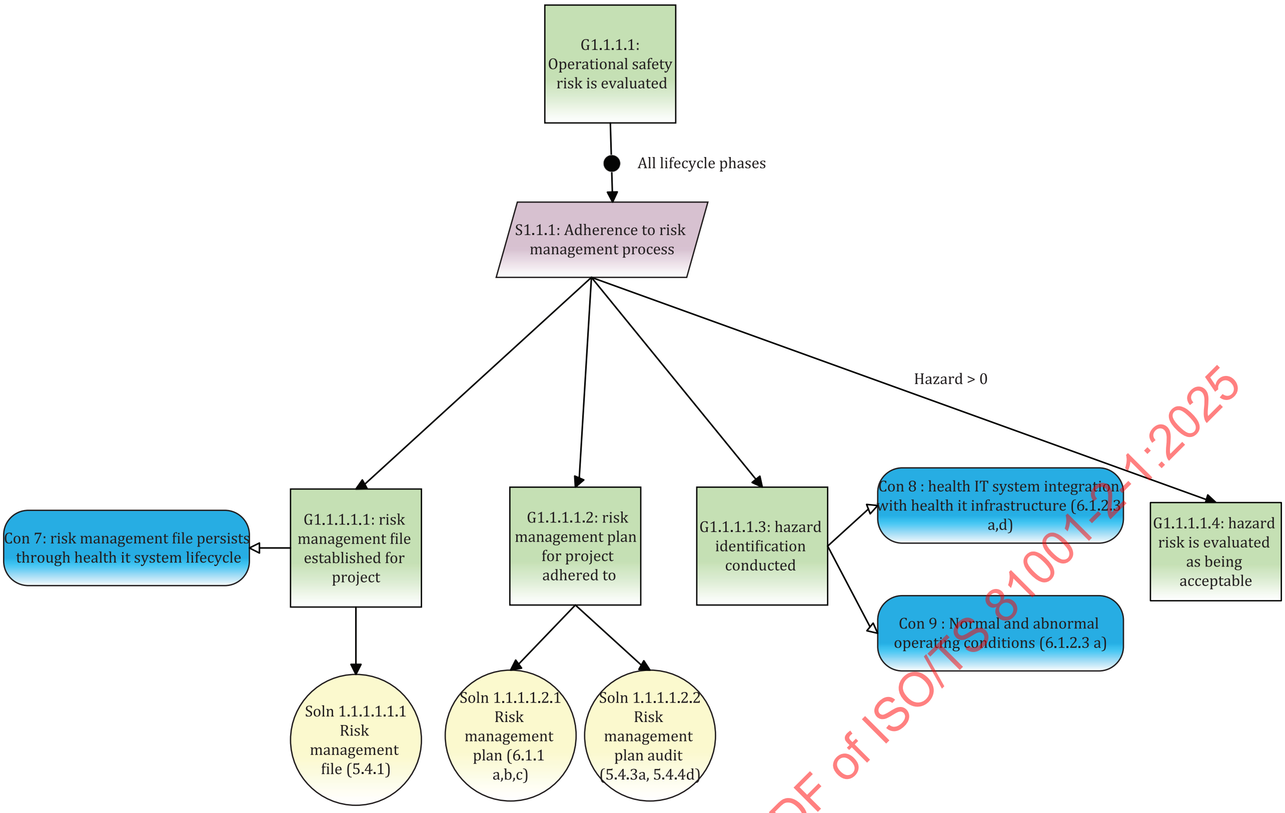
G1.1.1.1: Operational safety risk is evaluated
All lifecycle phases
S1.1.1: Adherence to risk management process
Hazard > 0
Con 7: risk management file persists through health it system lifecycle
G1.1.1.1.1: risk management file established for project
G1.1.1.1.2: risk management plan for project adhered to
G1.1.1.1.3: hazard identification conducted
Con 8 : health IT system integration with health it infrastructure (6.1.2.3 a,d)
Con 9 : Normal and abnormal operating conditions (6.1.2.3 a)
G1.1.1.1.4: hazard risk is evaluated as being acceptable
Soln 1.1.1.1.1.1 Risk management file (5.4.1)
Soln 1.1.1.1.2.1 Risk management plan (6.1.1 a,b,c)
Soln 1.1.1.1.2.2 Risk management plan audit (5.4.3a, 5.4.4d)

Figure B.4 — Goal G1.1.1.1

Figure B.5 supports Figure B.4 and establishes a sub goal that hazard identification activities have been conducted. Typical evidence artefacts are identified which substantiate this goal.

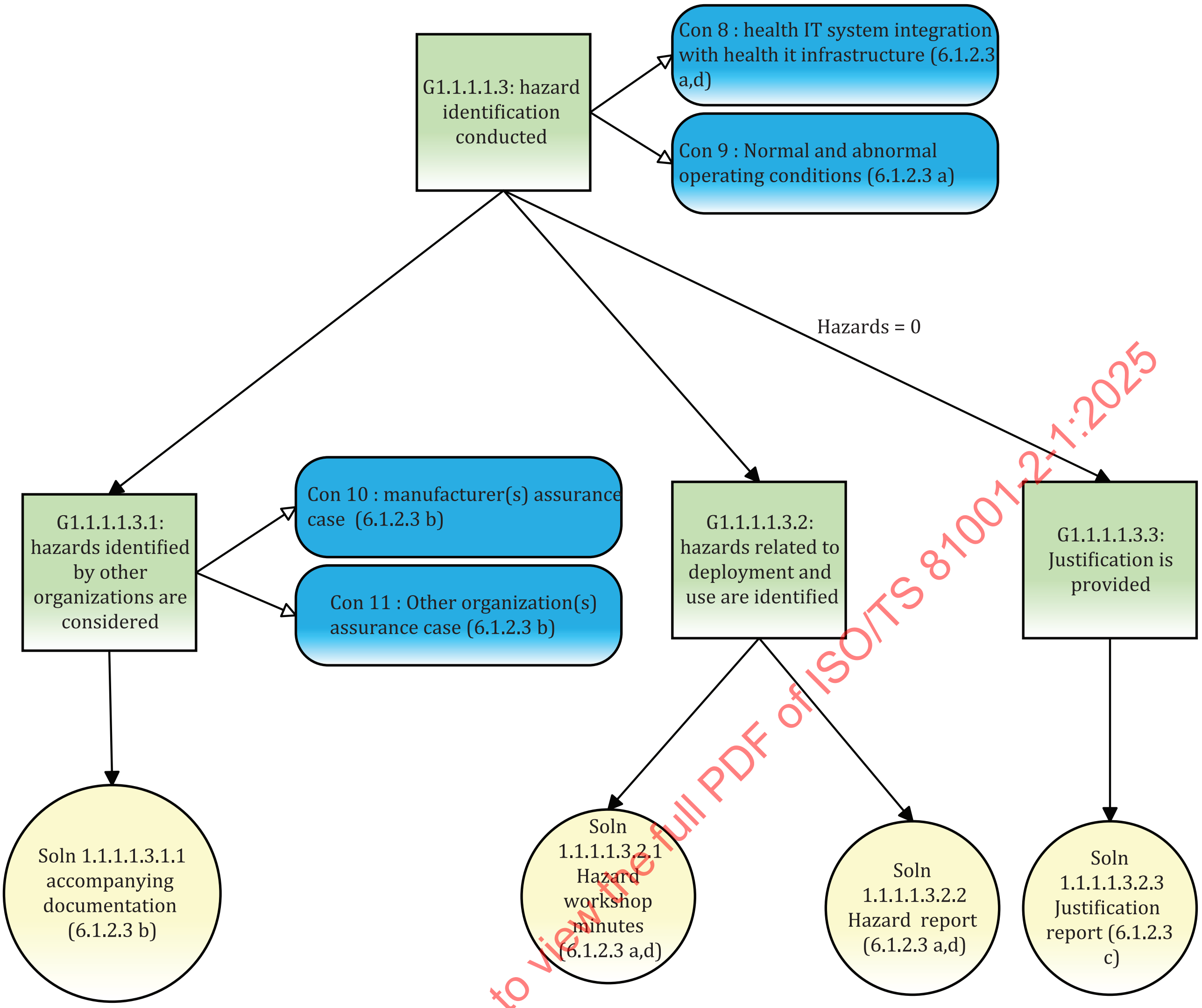
G1.1.1.1.3: hazard identification conducted
Con 8 : health IT system integration with health it infrastructure (6.1.2.3 a,d)
Con 9 : Normal and abnormal operating conditions (6.1.2.3 a)
Hazards = 0
G1.1.1.1.3.1: hazards identified by other organizations are considered
Con 10 : manufacturer(s) assurance case (6.1.2.3 b)
Con 11 : Other organization(s) assurance case (6.1.2.3 b)
G1.1.1.1.3.2: hazards related to deployment and use are identified
G1.1.1.1.3.3: Justification is provided
Soln 1.1.1.1.3.1.1 accompanying documentation (6.1.2.3 b)
Soln 1.1.1.1.3.2.1 Hazard workshop minutes (6.1.2.3 a,d)
Soln 1.1.1.1.3.2.2 Hazard report (6.1.2.3 a,d)
Soln 1.1.1.1.3.2.3 Justification report (6.1.2.3 c)

Figure B.5 — Goal G1.1.1.1.3

Figure B.6 supports Figure B.4 and establishes a sub goal that the hazard risk has been evaluated to be acceptable. Typical evidence artefacts are identified which substantiate this goal.

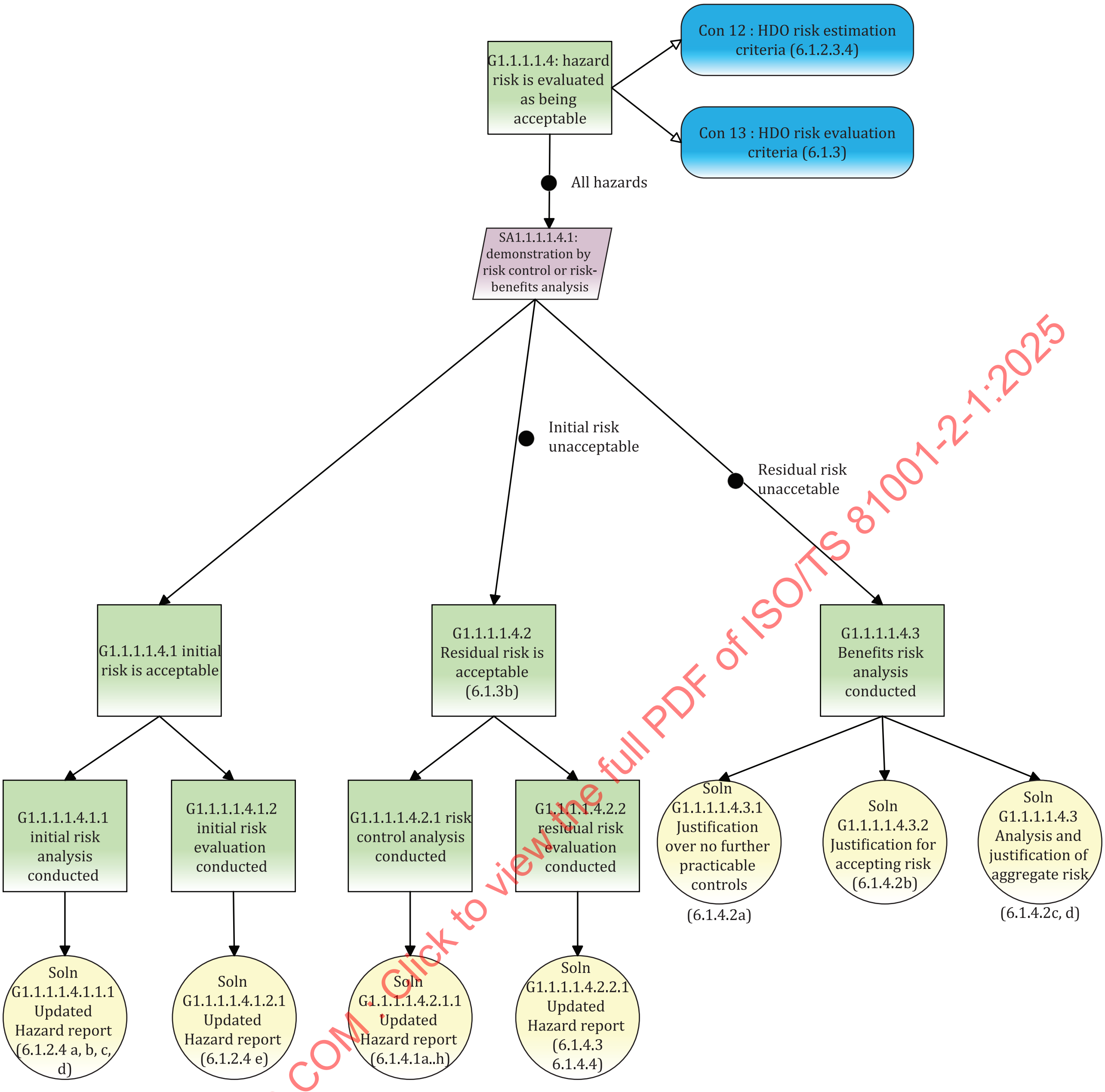
G1.1.1.1.4: hazard risk is evaluated as being acceptable
Con 12 : HDO risk estimation criteria (6.1.2.3.4)
Con 13 : HDO risk evaluation criteria (6.1.3)
All hazards
SA1.1.1.1.4.1: demonstration by risk control or risk-benefits analysis
Initial risk unacceptable
Residual risk unaccetable
G1.1.1.1.4.1 initial risk is acceptable
G1.1.1.1.4.2 Residual risk is acceptable (6.1.3b)
G1.1.1.1.4.3 Benefits risk analysis conducted
G1.1.1.1.4.1.1 initial risk analysis conducted
G1.1.1.1.4.1.2 initial risk evaluation conducted
G1.1.1.1.4.2.1 risk control analysis conducted
G1.1.1.1.4.2.2 residual risk evaluation conducted
Soln G1.1.1.1.4.3.1 Justification over no further practicable controls
(6.1.4.2a)
Soln G1.1.1.1.4.3.2 Justification for accepting risk (6.1.4.2b)
Soln G1.1.1.1.4.3 Analysis and justification of aggregate risk
(6.1.4.2c, d)
Soln G1.1.1.1.4.1.1 Updated Hazard report (6.1.2.4 a, b, c, d)
Soln G1.1.1.1.4.1.2.1 Updated Hazard report (6.1.2.4 e)
Soln G1.1.1.1.4.2.1.1 Updated Hazard report (6.1.4.1a..h)
Soln G1.1.1.1.4.2.2.1 Updated Hazard report (6.1.4.3 6.1.4.4)

Figure B.6 — Goal G1.1.1.1.4

Figure B.7 supports Figure B.2 and establishes a sub goal that the operational security risk of the HIT system is accepted by the HDO's top management. In practice, this is a repeat of G1.1.1 and its sub goals, but in the context of security risk. The impact of the security vulnerabilities or mitigations shall be considered from a hazard contribution perspective and included in the assurance case.

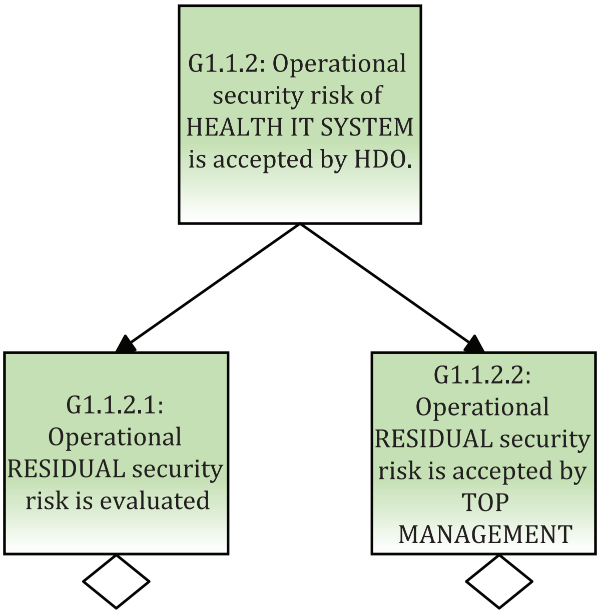
G1.1.2: Operational security risk of HEALTH IT SYSTEM is accepted by HDO.
G1.1.2.1: Operational RESIDUAL security risk is evaluated
G1.1.2.2: Operational RESIDUAL security risk is accepted by TOP MANAGEMENT

Figure B.7 — Goal G1.1.2

Figure B.8 supports Figure B.1 and establishes a sub goal that the manufacturer supports the HDO in meeting the requirements of IEC 80001-1:2021. Typical evidence artefacts are identified which substantiate this goal.

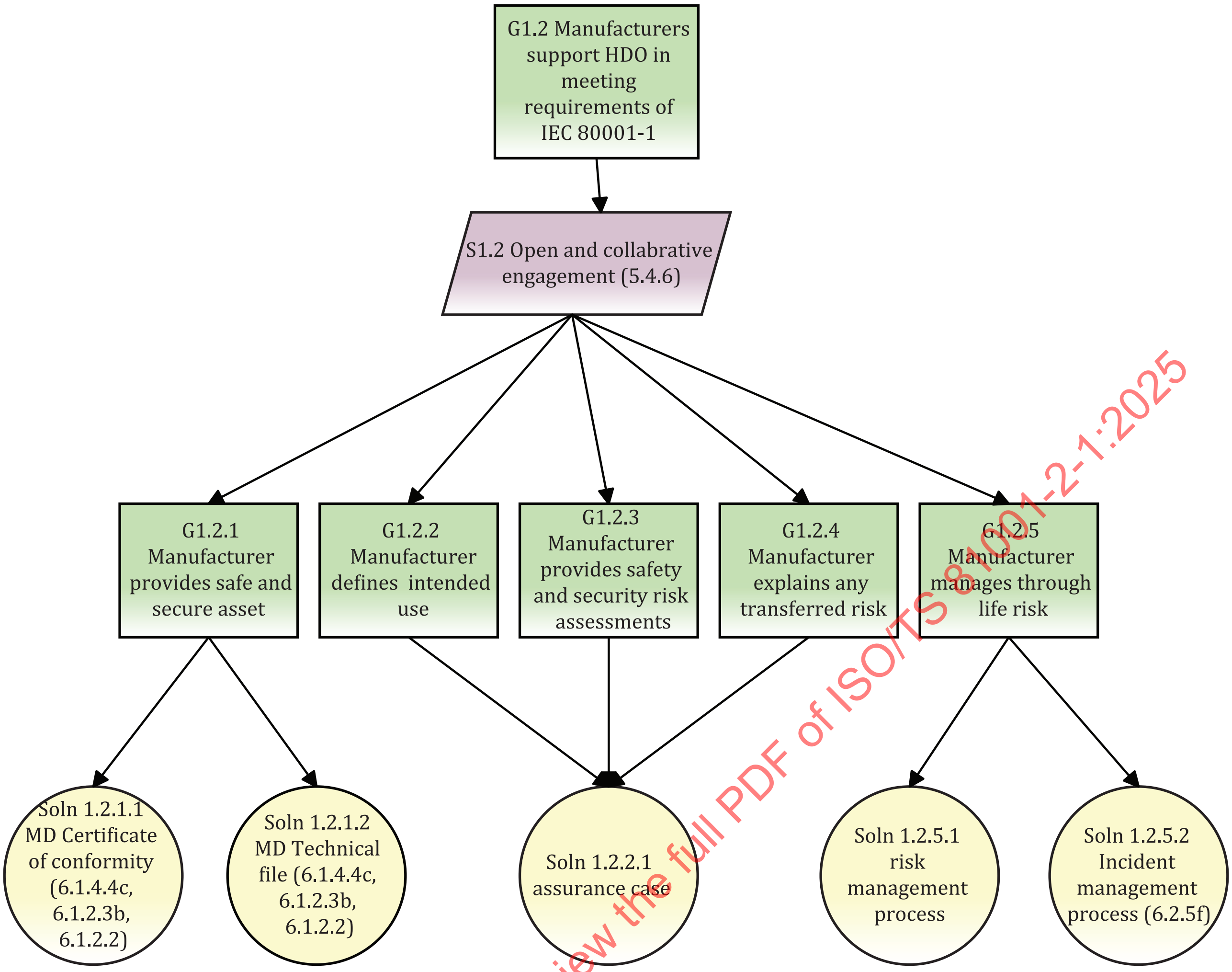
G1.2 Manufacturers support HDO in meeting requirements of IEC 80001-1
S1.2 Open and collabrative engagement (5.4.6)
G1.2.1 Manufacturer provides safe and secure asset
G1.2.2 Manufacturer defines intended use
G1.2.3 Manufacturer provides safety and security risk assessments
G1.2.4 Manufacturer explains any transferred risk
G1.2.5 Manufacturer manages through life risk
Soln 1.2.1.1 MD Certificate of conformity (6.1.4.4c, 6.1.2.3b, 6.1.2.2)
Soln 1.2.1.2 MD Technical file (6.1.4.4c, 6.1.2.3b, 6.1.2.2)
Soln 1.2.2.1 assurance case
Soln 1.2.5.1 risk management process
Soln 1.2.5.2 Incident management process (6.2.5f)

Figure B.8 — Goal G2.1

Annex C
(informative)

AI assurance case pattern

Figures C.1 to C.9 depict an assurance case, using GSN, that illustrates how the safety characteristics of an AI component can be demonstrated to be adequate from a perspective of intended use by an HDO. Tables C.1 to C.9 explain how particular elements of the assurance case support the top goal.

Figure C.1 establishes the overarching goal that the AI component is acceptably safe for intended use by the HDO. It defines the context in which this is claimed and that this is achieved through demonstration of safe component development and deployment

Table C.1 explains the relevance and the contribution of key components of the assurance case in achieving the top-level goal.

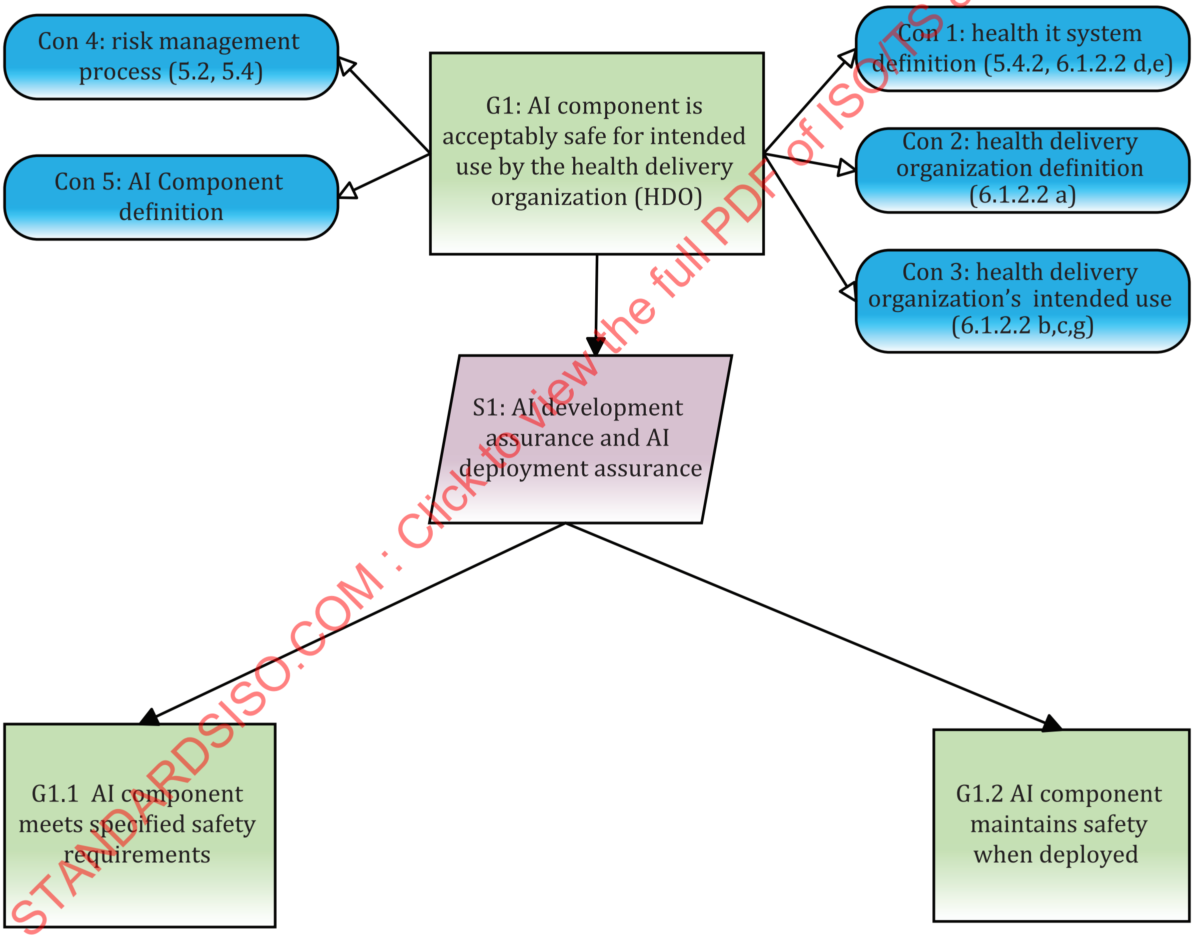
Con 4: risk management process (5.2, 5.4)
Con 5: AI Component definition
G1: AI component is acceptably safe for intended use by the health delivery organization (HDO)
Con 1: health it system definition (5.4.2, 6.1.2.2 d,e)
Con 2: health delivery organization definition (6.1.2.2 a)
Con 3: health delivery organization’s intended use (6.1.2.2 b,c,g)
S1: AI development assurance and AI deployment assurance
G1.1 AI component meets specified safety requirements
G1.2 AI component maintains safety when deployed

Figure C.1 — AI assurance case pattern

Table C.1 — AI assurance case narrative

Assurance case component	Explanation
G1	Establishes a top-level claim that the AI component is safe to use for its purpose at the point of care delivery. This claim is established in the context of (Con 1 to 5) that define or describe artefacts that define the scope and boundary of the assurance case.
S1	Defines the way in which G1 will be achieved, i.e. by demonstrating sufficiency in both the AI component development and deployment assurance.
G1.1	Establishes a claim that the AI component meets its safety requirements which have been derived from system level safety requirements (Con 6). The AI component manufacturer would be responsible for substantiating this element of the assurance case. The establishment of this requirement and the sharing of the conclusions could be achieved through a responsibility agreement between the HDO and manufacturer.
G1.2	Establishes a claim that the AI component continues to achieve its safety requirements when it is deployed and used in a clinical setting. The HDO would be responsible for substantiating this element of the assurance case.

Figure C.2 supports Figure C.1 and establishes a goal that the AI component meets the safety requirements allocated to it. This is argued through adherence to a systematic assurance process.

Table C.2 explains the relevance and the contribution of key components of the assurance case in achieving this goal.

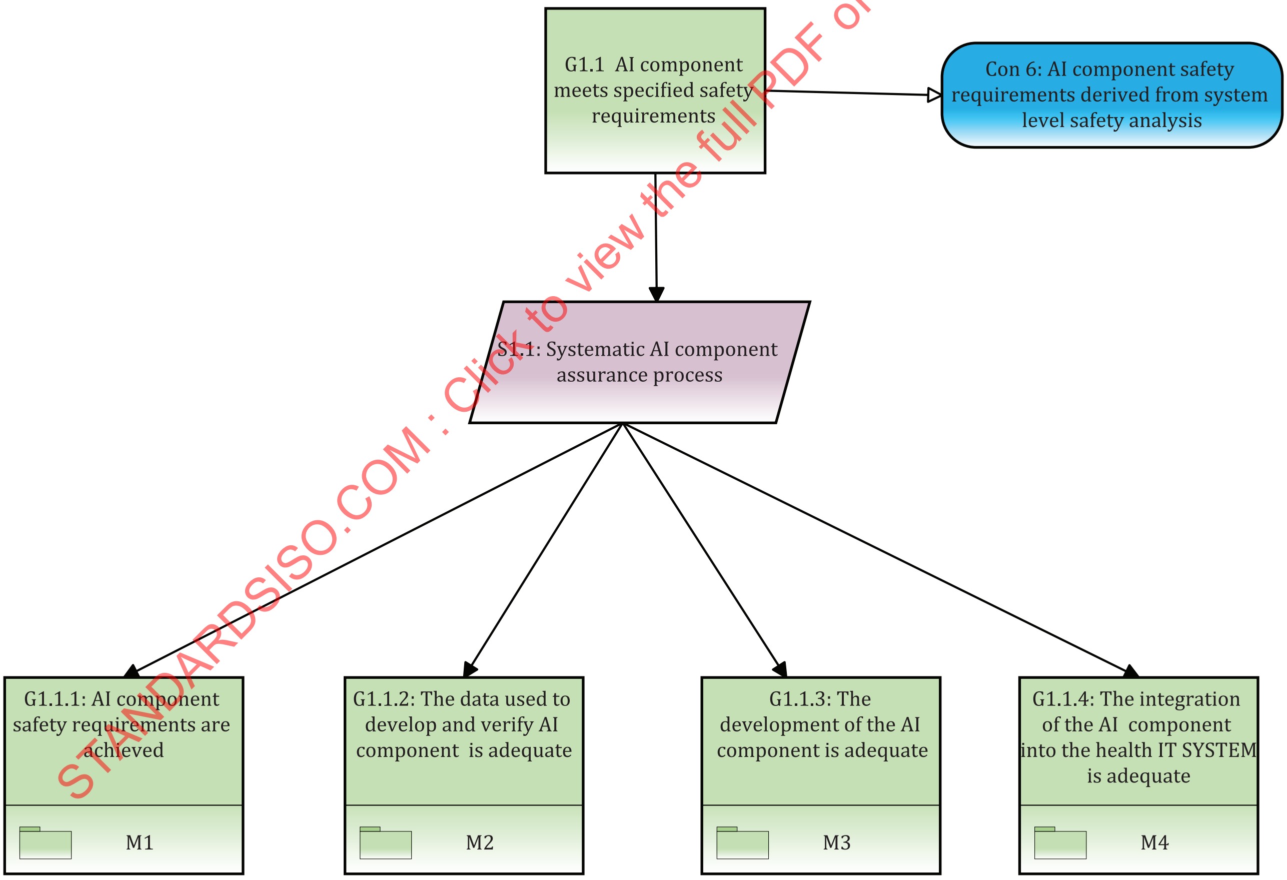
G1.1 AI component meets specified safety requirements
Con 6: AI component safety requirements derived from system level safety analysis
S1.1: Systematic AI component assurance process
G1.1.1: AI component safety requirements are achieved
M1
G1.1.2: The data used to develop and verify AI component is adequate
M2
G1.1.3: The development of the AI component is adequate
M3
G1.1.4: The integration of the AI component into the health IT SYSTEM is adequate
M4

Figure C.2 — AI assurance case pattern (G1.1)

Table C.2 — AI assurance case narrative (G1.1)

Assurance case component	Explanation
G1.1	Establishes a claim that the AI component meets its safety requirements which have been derived from system level safety requirements (Con 6).
S1.1	Defines the way in which G1 will be achieved, i.e. by demonstrating that a systematic approach to AI component assurance has been undertaken. This strategy considers themes of assurance (G1.1.1 to G1.1.4) which are considered to contribute to G1.1. Further reading is available[8]

Figure C.3 supports Figure C.2 and establishes a goal that the AI component achieves its safety requirements. This is argued through validation of allocated safety requirements and verification of AI characteristics against these requirements. Accomplishment is achieved through provision of relevant verification and validation (V&V) results.

Table C.3 explains the relevance and the contribution of key components of the assurance case in achieving this goal.

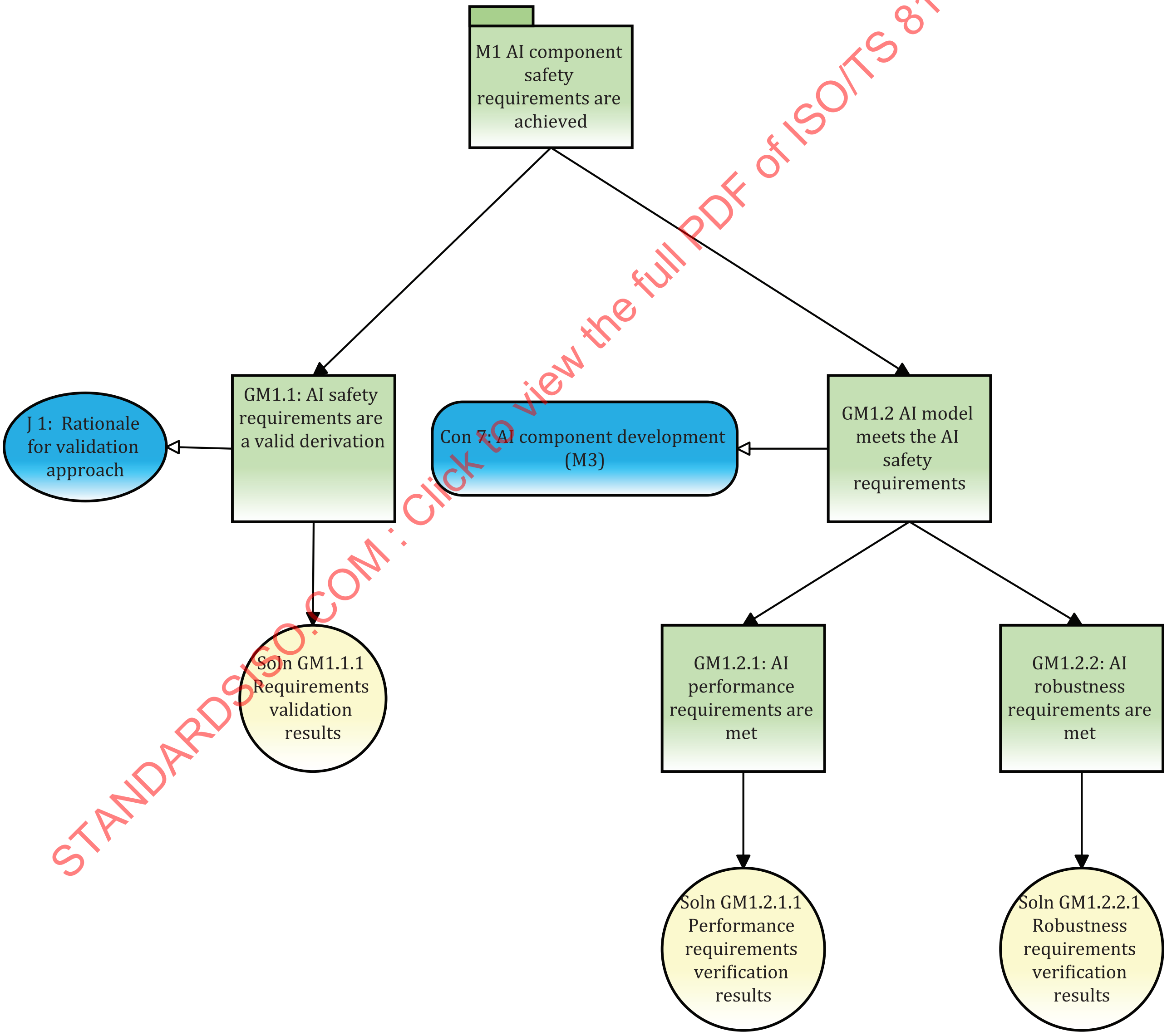
M1 AI component safety requirements are achieved
J 1: Rationale for validation approach
GM1.1: AI safety requirements are a valid derivation
Con 7: AI component development (M3)
GM1.2 AI model meets the AI safety requirements
Soln GM1.1.1 Requirements validation results
GM1.2.1: AI performance requirements are met
GM1.2.2: AI robustness requirements are met
Soln GM1.2.1.1 Performance requirements verification results
Soln GM1.2.2.1 Robustness requirements verification results

Figure C.3 — AI assurance case pattern (M1)

Table C.3 — AI assurance case narrative (M1)

Assurance case component	Explanation
G1.1.1 / M1	Establishes a claim that the AI component meets the safety requirements allocated to it from the system level safety analysis. The strategy to achieve this is demonstrated by demonstrating that the allocated safety requirements are valid (GM1.1) and that the AI model meets these requirements (GM1.2).
GM1.1	Establishes a claim that the safety requirements that have been allocated to the AI model are valid. To support this, the validation process will need to be explained and justified as being appropriate (J1). Achievement of GM1.1 is through Soln GM1.1.1 which would provide evidence of the requirements validation exercise having been completed.
GM1.2	Establishes a claim that the data requirements required to develop a safe and high performing AI component have met. Achievement of GM2.2 is through Soln GM2.2.1 to Soln GM2.2.4 which would provide evidence that the data characteristics relevant to the AI component's development and assurance have been realised. Further solutions addressing other characteristics may be added to the evidence base; this would be dependent on the nature of the AI model and the context it is intended to be used in.

Figure C.4 supports Figure C.2 and establishes a goal that the data used to develop the AI component is adequate. This is argued through demonstration of independence across datasets and validation of key data characteristics that can have a detrimental effect on the AI components safety characteristics. Accomplishment is achieved through provision of relevant validation results.

Table C.4 explains the relevance and the contribution of key components of the assurance case in achieving this goal.

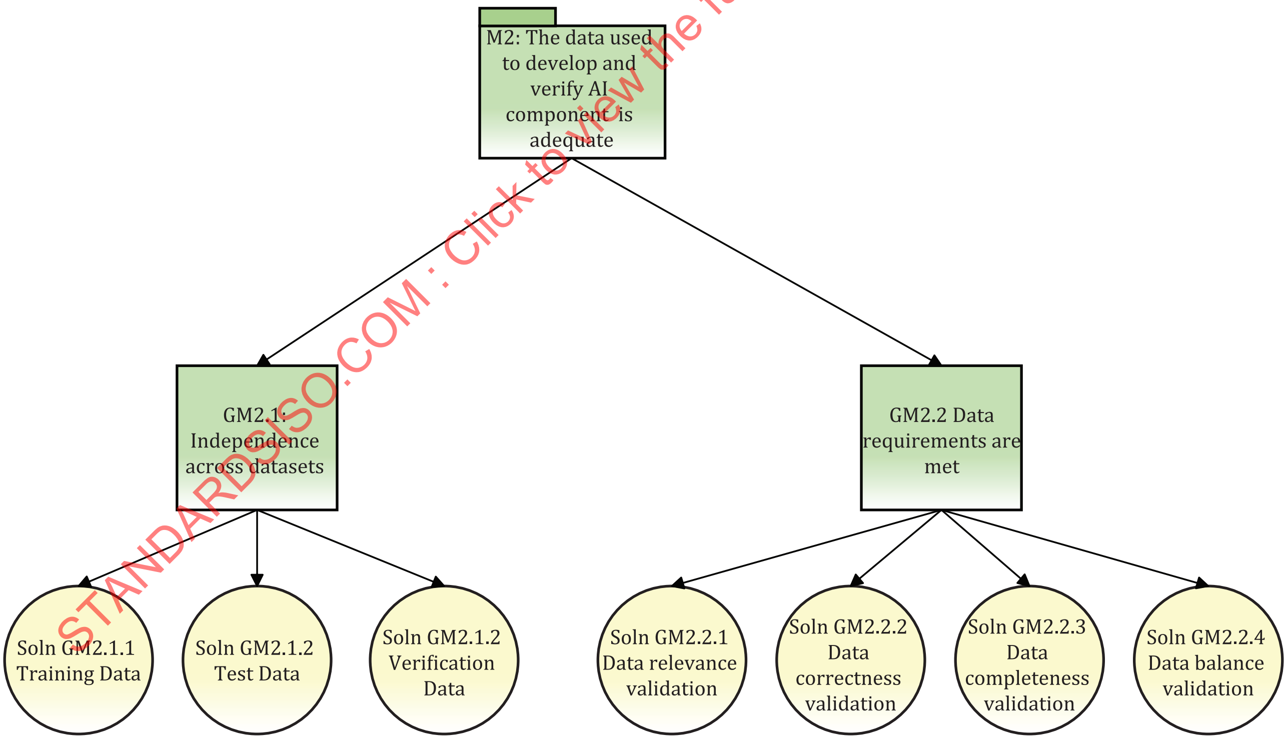
M2: The data used to develop and verify AI component is adequate
GM2.1: Independence across datasets
GM2.2 Data requirements are met
Soln GM2.1.1 Training Data
Soln GM2.1.2 Test Data
Soln GM2.1.2 Verification Data
Soln GM2.2.1 Data relevance validation
Soln GM2.2.2 Data correctness validation
Soln GM2.2.3 Data completeness validation
Soln GM2.2.4 Data balance validation

Figure C.4 — AI assurance case pattern (M2)

Table C.4 — AI assurance case narrative (M2)

Assurance case component	Explanation
G1.1.2 / M2	Establishes a claim that the data used in the development of the AI component is adequate. The strategy to achieve this claim is obvious from the GSN model, thus it has not been explicitly depicted. Adequacy will be demonstrated by demonstrating independence across data sets (GM2.1) and showing that relevant data characteristics have been met (GM2.2). An instance of this module would be instantiated for each AI component.
GM2.1	Establishes a claim that there is independence in the data that is used to train, test, and verify the AI component. Common datasets cannot be used to achieve these three key development activities; no evidence would be generated to indicate that the AI component performs as intended when exposed to data that it has not seen before. Achievement of GM2.1 is through Soln GM2.1.1 to GGM2.1.3, which would extend to explain the provenance and source of the datasets. In practice it can be necessary to generate synthetic data that is representative of ground truth data.
GM2.2	Establishes a claim that the data requirements required to develop a safe and high performing AI component have been met. Achievement of GM2.2 is through Soln GM2.2.1 to GM2.2.4 which would provide evidence that the data characteristics relevant to the AI component's development and assurance have been realized. Further solutions addressing other characteristics may be added to the evidence base; this would be dependent on the nature of the AI model and the context it is intended to be used in.

Figure C.5 supports Figure C.2 and establishes a goal that the development of the AI component is adequate. This is argued through demonstration that the development process is appropriate for the intended use of the AI component and that the developed AI component achieves its safety requirements. Accomplishment is achieved through provision of relevant justifications and validation results.

Table C.5 explains the relevance and the contribution of key components of the assurance case in achieving this goal.

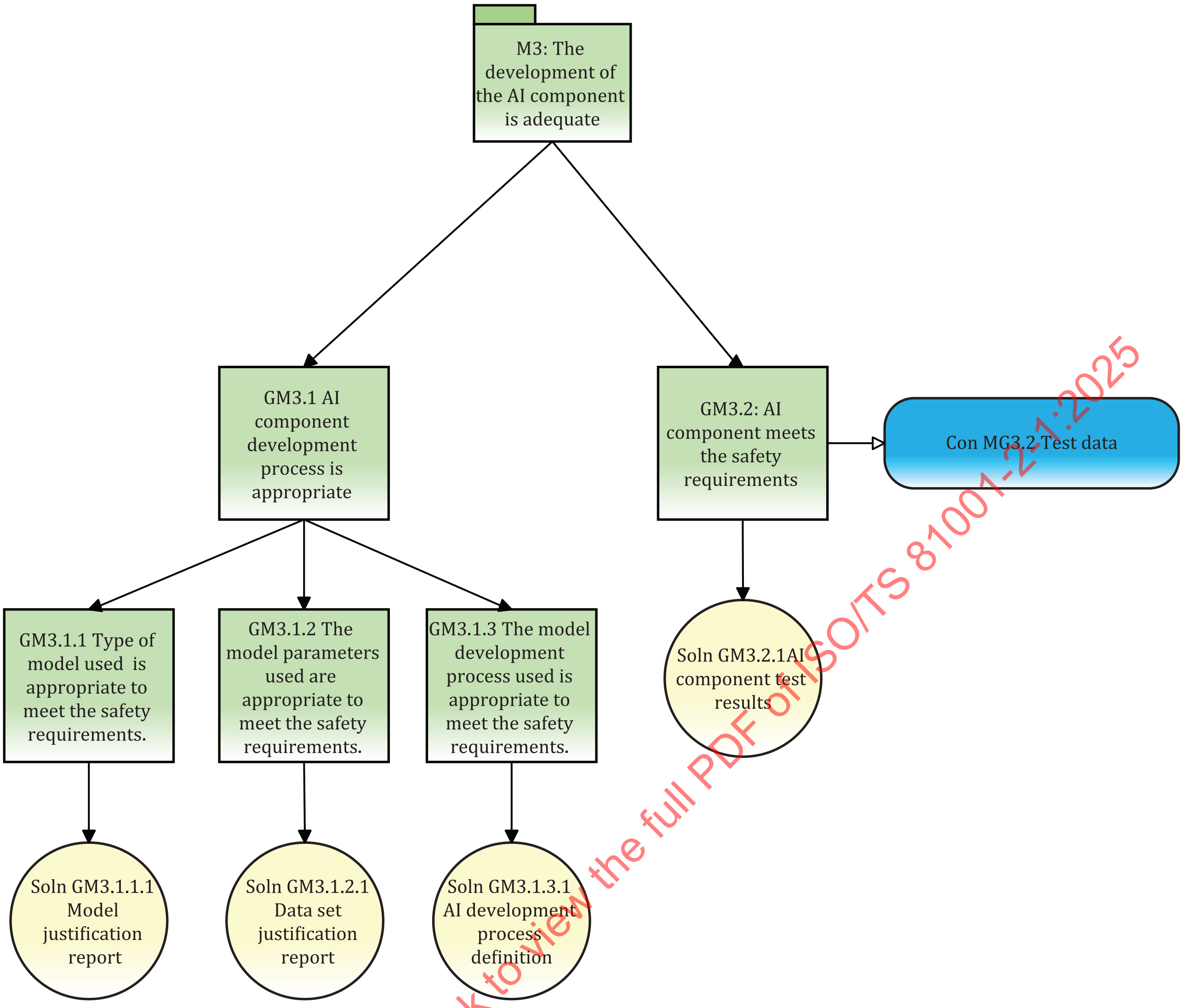
M3: The development of the AI component is adequate
GM3.1 AI component development process is appropriate
GM3.2: AI component meets the safety requirements
Con MG3.2 Test data
GM3.1.1 Type of model used is appropriate to meet the safety requirements.
GM3.1.2 The model parameters used are appropriate to meet the safety requirements.
GM3.1.3 The model development process used is appropriate to meet the safety requirements.
Soln GM3.2.1AI component test results
Soln GM3.1.1.1 Model justification report
Soln GM3.1.2.1 Data set justification report
Soln GM3.1.3.1 AI development process definition

Figure C.5 — AI assurance case pattern (M3)

Table C.5 — AI assurance case narrative (M3)

Assurance case component	Explanation
G1.1.3 / M3	Establishes a claim that the developed model is adequate to meet the derived and allocated safety requirements. Adequacy will be demonstrated by establishing that the development process is appropriate for the AI component's intended purpose (GM3.1) and that testing provides evidence that the safety requirements are achieved (GM3.2). An instance of this module would be instantiated for each AI component.
GM3.1	Establishes a claim that the development process is appropriate for the AI component's intended purpose. This is achieved through a justification that the model type chosen is appropriate for the intended purpose of the AI component (GM3.1.1), that the data parameters used to train the model are appropriate (GM3.1.2) and that model development process is appropriate to meet the allocated safety requirements (GM3.1.3). These sub goals are substantiated through a justification of the related activities.
GM3.2	Establishes a claim, in the context of specified test data, that the developed AI component meets its allocated safety requirements. Achievement of GM3.2 is through Soln GM3.2.1 which provides the test evidence.