ISO/IEC ~~JTC 1 /SC 7 N2XXXX~~

~~Date:2024-07-15~~

~~DIS~~ ISO/IEC ~~DIS~~ FDIS 24760-~~-~~2:2024 ~~(E(en)~~

ISO/IEC JTC 1/SC 27/WG 5

Secretariat: DIN

Date: 2024-11-26

IT Security and Privacy— — A framework for identity management— — Part 2: Reference architecture and requirements

Sécurité informatique et Protection de la vie privée—Cadre pour la gestion d'identité——Partie 2: Architecture de référence et exigences

~~*Partie 2: Architecture de référence et exigences*~~

Formatted: Centered

Style Definition: Heading 1
Style Definition: Heading 2
Style Definition: Heading 3
Style Definition: Heading 4
Style Definition: Heading 5
Style Definition: Heading 6
Style Definition: Default Paragraph Font
Style Definition: ANNEX
Style Definition: List Paragraph
Style Definition: Note: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: 1.7 cm, Left + Not at 2 cm
Style Definition: Body Text Indent 2
Style Definition: Body Text Indent 3
Style Definition: AMEND Terms Heading
Style Definition: AMEND Heading 1 Unnumbered
Style Definition: IneraTableMultiPar: Font: Font color: Black, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Top: 1.4 cm, Bottom: 0.5 cm, Section start: New page
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: French (Switzerland)
Formatted: Font: Bold, Not Italic, French (Switzerland)

Formatted: Centered

Formatted

Contents~~—~~

Formatted ... (repeated 70 times)
Field Code Changed ... (repeated 8 times)

Formatted: Font: 11 pt, French (Switzerland)
Formatted: Centered
Formatted: Font: 11 pt, French (Switzerland)
Formatted: Font: 11 pt, French (Switzerland)
Formatted: English (United States), Ligatures: None
Formatted: English (United States), Ligatures: None
Formatted: English (United States), Ligatures: None
Formatted: English (United States), Ligatures: None
Formatted: English (United States), Ligatures: None
Formatted: English (United States), Ligatures: None
Field Code Changed
Formatted: English (United States), Ligatures: None
Formatted: English (United States), Ligatures: None
Formatted: English (United States), Ligatures: None
Field Code Changed
Formatted: English (United States), Ligatures: None
Field Code Changed
Formatted: English (United States), Ligatures: None
Formatted: English (United States), Ligatures: None
Formatted: Tab stops: 18.18 cm, Right,Leader: ...
Formatted: Normal, Centered, Space After: 24 pt, Tab stops: 17.2 cm, Right

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 ~~documents~~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~~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~~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~~www.iso.org/iso/foreword.html. In the IEC, see ~~www.iec.ch/understanding-standards~~www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 24760-2:2015), which has been technically revised.

The main changes are as follows:

— in Clause 3, the definitions of terms from ISO/IEC 24760-1 was removed;

— to address the emerging concept of mobile identity, the term “principal’s private IMS” (PPI) was added in Clauses 3, 4, and described in 5.4.2, 5.4.3 and 5.4.6;

— some of the content of Clause 5 was moved to Clauses 6 and 7;

— former Annex A has been deleted and the existing annexes have been relabelled.

A list of all parts in the ISO/IEC ISO/IEC 24760 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~~www.iso.org/members.html and www.iec.ch/national-committees.

Formatted: Font: Not Italic
Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Font: Italic
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Default Paragraph Font
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: cite_app
Formatted: cite_app
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: std_publisher
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear

Formatted: Font: 11 pt, French (Switzerland)

Formatted: Centered

Formatted: Font: 11 pt, French (Switzerland)

Formatted: Font: 11 pt, French (Switzerland)

Formatted: Normal, Centered, Space After: 24 pt, Tab stops: 17.2 cm, Right

Introduction

Data processing systems commonly gather a range of information on its users, which can include people, pieces of equipment, or pieces of software connected to the equipment. Based on the information gathered on user identity, these data processing systems make decisions that can impact how users access to IT resources.

To address the need to efficiently and effectively implement systems that make identity-based decisions, this document specifies a framework for the issuance, administration and use of data. This framework serves to characterize individuals, organizations, or information technology components, which operate on behalf of individuals or organizations.

For many organizations, the proper management of identity information is crucial for maintaining the security of the organizational processes. For individuals, correct identity management is important for protecting privacy.

The ISO/IEC 24760 series specifies fundamental concepts and operational structures for identity management and provides a framework on which information systems can meet business, contractual, regulatory, and legal obligations.

This document defines a reference architecture for identity management including interrelationships. These architectural elements are described in respect to identity management deployments models. This document also specifies requirements for the design and implementation of an identity management system so that it can meet the objectives of stakeholders involved in the deployment and operation of identity management.

This document is intended to provide a foundation for the implementation of other international standards related to identity information processing such as ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 29115, and ISO/IEC 29146.

This document is not a management system standard (MSS).

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Body Text, Space After: 0 pt, Tab stops: Not at 0.7 cm + 1.4 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm

IT security and Privacy — A framework for identity management— — Part 2: Reference architecture and requirements

1 Scope

This document:

— provides guidelines for the implementation of systems for the management of identity information~~, and~~;

— specifies requirements for the implementation and operation of a framework for identity management~~.~~;

~~This document~~ — is applicable to any information system where information relating to identity is processed or stored~~.~~;

— is considered to be a horizontal document for the following reasons:

  — it applies concepts such as distinguishing the term "identity" from the term "identifier" on the implementation of systems for the management of identity information and on the requirements for the implementation and operation of a framework for identity management,

  — it provides an important contribution to assess identity management systems with regard to their privacy-friendliness and their ability to assure the relevant attributes of an identity, and consequently it provides a foundation and a common understanding for any other standard addressing identity, identity information, and identity management.

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/IEC 24760~~-~~-1, *IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*

ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24760~~-1and-~~1 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~~https://www.iso.org/obp

Formatted: Font: 11.5 pt, Bold
Formatted: Font: Bold
Formatted: Font: Bold
Formatted: Normal, Line spacing: Exactly 12 pt
Formatted: Font: 12 pt, Bold
Formatted: Font: Bold
Formatted: Font: 12 pt, Bold
Formatted: Centered
Formatted: List Continue 1, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Widow/Orphan control, Tab stops: Not at 1 cm
Formatted: List Continue 1, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Widow/Orphan control
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...
Formatted: English (United Kingdom)
Formatted ...
Formatted ...

— IEC Electropedia: available at ~~https://www.electropedia.org/~~https://www.electropedia.org/

3.1
documented design

authoritative description of structural, functional, and operational system aspects

Note 1 to entry: A documented design is the documentation created to serve as guidance for the implementation of an Information and Communication Technology (ICT) system.

Note 2 to entry: A documented design typically includes the description of a concrete architecture of the ICT system.

3.2
identity management authority

entity responsible for setting and enforcing operational policies for an identity management system

Note 1 to entry: An identity management authority typically commissions the design, implementation, and deployment of an identity management system.

EXAMPLE:~~—~~ The executive management of a company deploying an identity management system in support of its services.

3.3
invalidation

process performed in an identity management system when a particular attribute is no longer valid for a particular entity to mark the attribute invalid for future use

Note 1 to entry: Invalidation of attributes can be part of updating the attribute value, for instance, with a change of address.

Note 2 to entry: Invalidation typically takes place for an attribute that is determined as no longer valid before the end of a validity period that had previously been associated with it.

Note 3 to entry: The term “revocation” is commonly used for invalidation of attributes that are credentials.

Note 4 to entry: Invalidation typically happens immediately after the determination that an attribute is no longer valid for a particular entity.

3.4
regulatory body

formally recognized organization tasked and empowered by law, regulation, or agreement to supervise the operation of identity management systems

3.5
stakeholder

role, position, individual, organization, or classes thereof, having an interest, right, share, or claim, in an entity of interest

[SOURCE: ISO/IEC/IEEE 42010:2022, 3.17~~]~~, modified — the Example has been removed.]

3.6
principal’s private identity management system
PPI

identity management system holding identity information for a single principal, operated by, or under exclusive control of, this principal

Note 1 to entry: The wording “mobile identity” has been used to, among other concepts, refer to a principal’s private identity management system, e.g. as implemented on a mobile phone or as a dedicated processing token.

Formatted: English (United Kingdom)

Formatted: Font: Cambria, English (United Kingdom)

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Font: Cambria, Font color: Auto, English (United Kingdom)

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

4 Symbols and abbreviated terms

ICT	information and communication technology
IMS	identity management system
PII	personally identifiable information
PPI	principal's private identity management system
UML	Unified modellingunified modeling language

5 Reference architecture

5.1 General

This clause describes the architectural elements for identity management and the relationships between these elements.

The documented design for the architecture of identity management should be based on ISO/IEC/IEEE 42010 and address the primary concerns of this system, which can be either one or both of the following:

a) managing identity information for the members of an organization, (Clause 6);

b) managing identity information for entities outside an organization (Clause 7).

NOTE The reference architecture and architecture description specified in this document are based on ISO/IEC/IEEE 42010.

The documented design for the architecture of an identity management system should specify the system in its deployed context based on stakeholders and actors defined in this document. Business-level actors are stakeholders. Some stakeholders do not interact with the system. The documented design shall address requirements for both actor and non-actor stakeholders. The documented design shall exhaustively describe the actors.

A documented design for identity management should use applicable language to describe the reference architecture; components and functions of this architecture should be labelled followingaccording to the terms defined in the ISO/IEC 24760 (all parts).series.

This clause provides an overview of the components that can be present in one or more of the architectural views that can be specified in a documented design including:

— stakeholders (5.3),(5.3),

— actors (5.4),(5.4), and

— processes and services (5.5). (5.5).

Sub-clause 5.6 presents two commonlyTwo common viewpoints for identity management are presented in 5.6.

5.2 Deployment scenarios

An identity management system can be deployed according to various scenarios. A deployment scenario impacts governance of the identity management system. The deployment scenario determines the trust relationships that exist between parties involved in operating and governing the identity management system.

Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt
Formatted: Centered, Space After: 30 pt, Line spacing: Exactly 11 pt
Formatted: Font: 11.5 pt
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Centered, Space After: 24 pt, Tab stops: 17.2 cm, Right

A deployment scenario can be chosen when extending an existing identity management system. An extension deployment model can be different from the original or enterprise deployment model.

The different deployment scenarios that can be used to implement an identity management system include:

— the enterprise scenario ~~(6.3);~~(6.3);

— the federated scenario ~~(7.3.1);~~(7.3.1);

— the service scenario ~~(7.3.2);~~(7.3.2);

— the federated scenario as applied as a service ~~(7.3.3).~~(7.3.3).

5.3 Stakeholders

5.3.1 General

The documented design can recognize the following direct and indirect stakeholders:

— principal,

— identity management authority,

— identity information authority,

— relying party,

— regulatory body,

— auditor,

— assessor,

— cloud service provider, and

— consumer/citizen representative or advocate.

Each stakeholder performs a separate function in the identity management system. These functions imply specific responsibilities and liabilities.

NOTE 1 The purpose of the deployment of an identity management system, and the regulatory environment of that deployment, indicates the involvement of stakeholders.

Stakeholders in a particular identity management system can be affiliated with different commercial or public organizations with their interests in the system shaped by this affiliation. As the information about the system available to different stakeholders can be different, interactions between stakeholders should be based on explicitly established trust relations.

The documented design shall specify concrete representations of its stakeholders and actors as defined in 5.3 and 5.4, respectively. The documented design can add additional stakeholders or actors. It may also specify the stakeholders and actors identified in 5.3 and 5.4 with multiple distinct representations.

Stakeholders as specified in this document can also be actors. Non-actor stakeholders are a regulatory body and a consumer/citizen representative or advocate.

Concerns of stakeholders in an identity management system are described in ~~the following sub-clauses~~5.3.2 and 5.3.7 and should be addressed in the documented design, implementation and operation of the system.

Formatted: Widow/Orphan control, Tab stops: Not at 1 cm

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Formatted: Pattern: Clear

Formatted: Pattern: Clear

NOTE 2 Concerns expressed for each type of stakeholder are taken into consideration with references in developmentsofwhen developing Clauses 6 and 7. The same references can also be used in the documented designwhen documenting a reference architecture.

5.3.2 Principal

Concerns of a principal in an identity management system include:

— correctness of the identity information collected, processed and stored (can be referenced as ""data correctness");

— minimization of the identity information collected, processed and stored by the identity management system (can be referenced as "Data minimisation"data minimization");

— minimization of the identity information usage by the identity management system in its domain of applicability (can be referenced as "Information"information sharing minimization");

— ability of different relying parties to correlate identity information for a single principal (can be referenced as "Principal"principal correlation");

— ability of a relying party to positively link the principal with their recorded identity information received to identity information that it has already stored, e.g. a user account (can be referenced as ""correct authentication");

— errors in identification including false negative and false positive identification, and the detection and handling of errors (can be referenced as ""correct identification");

— knowledge of and consent to, identity information sharing with third parties (can be referenced as "Informationinformation and consent");

— being correctly represented by identity information which is captured, processed or stored (can be referenced as ""representative information");

— correctness of operations in the delivery of services and the access to resources made available based on the attributes presented in a specific situation (can be referenced as "Correct"correct operation");

— collecting, processing and storage of identity information only occurs with its informed consent (can be referenced as ""processing consent"),

— equitable treatment in its interactions with the system (can be referenced as ""equitable");

— an easily understandable, effective, appropriate user interface (can be referenced as "Understandable"understandable").

NOTE 3 A concern of a principal about how a third-party service uses identity information obtained from the identity management system is not a concern about the identity management system itself. Therefore, such a concern is not addressed explicitly in the documented design.

5.3.3 Identity management authority

Concerns of the identity management authority in an identity management system include:

— the definition of identity management objectives for the domain(s) served by the identity management system (can be referenced as ""defined objectives");

Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt
Formatted: Centered, Space After: 30 pt, Line spacing: Exactly 11 pt
Formatted: Font: 11.5 pt
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Default Paragraph Font
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Centered, Space After: 24 pt, Tab stops: 17.2 cm, Right

— specification of policies to maintain identity management objectives for the domain(s) served by the identity management system (can be referenced as ~~"~~"policies specified");

— fulfilment of the business objectives of the identity management system with respect to principals and users of identity information (can be referenced as ~~"~~"meeting user objectives");

— fulfilment of the business objectives of relationships with other identity management (can be referenced as ~~"~~"meeting third party objectives");

— accuracy of the identity information provided by each principal as pertaining to that principal and to a specific level of assurance (can be referenced as ~~"~~"correct information");

— ~~-~~compliance with regulation (can be referenced as ~~"~~"compliance").

5.3.4 Identity information authority

Concerns of an identity information authority in an identity management system include:

— completeness, correctness and freshness of the identity information (can be referenced as ~~"~~"data quality");

— meeting requirements from relying parties (can be referenced as ~~"~~"meeting needs of relying parties");

— effectiveness of the cryptographic methods to assert the identity information (can be referenced as ~~"~~"appropriate assertion");

— effectiveness of the cryptographic methods to de-identify the identity information (can be referenced as ~~"~~"effective de-identification");

— compliance with regulation (can be referenced as ~~"~~"compliance"); and

— meeting business obligations with principals (can be referenced as ~~"~~"meeting principal objectives").

5.3.5 Relying party

Concerns of a relying party in an identity management system include:

— confidentiality, availability and integrity, and applicability to a principal of identity information (can be referenced as ~~"~~"required identity information");

— provisioning of accurate identity information pertaining to relevant principals at the required level of assurance (can be referenced as ~~"~~"quality of information");

— effective, documented and secure interfaces (can be referenced as ~~"Usable~~"usable interfaces");

— conformance to regulation applicable to its operations (can be referenced as ~~"~~"compliance");

— effective mechanism and procedures for auditing (can be referenced as ~~"~~"auditing").

5.3.6 Regulatory body

As an external independent organization, concerns of a regulatory body in an identity management system include:

— the proper documentation of operating policies (can be referenced as ~~"~~"documented policies");

— correctness of operation, in particular, in applying operational polices (can be referenced as ~~"Correct~~"correct operation");

Formatted: Widow/Orphan control, Tab stops: Not at 1 cm