ISO/IEC JTC 1/SC 27 N19836

REPLACES: N19529

ISO/IEC JTC 1/SC 27

Information security, cybersecurity and privacy protection

Secretariat: DIN, Germany

DOC. TYPE:	**NP ballot**
TITLE:	**New work item proposal on Information security – Security techniques – Ontology for ICT Trustworthiness Assessment**
SOURCE:	**58th SC 27/WG 3 meeting (April 2019)**
DATE:	**2019-07-12**
PROJECT:	**NP**
STATUS:	**In accordance with Resolution 2 (contained in SC 27 N19900) of the 31st SC 27 Plenary meeting held in Tel-Aviv, Israel, 2019-04-08/09, this document is re-circulated to the SC 27 National Bodies for a 12-week NP letter ballot and to JTC 1 for a concurrent review. P-Members of SC 27 are requested to submit their votes on this document via the SC 27 e-balloting website at http://isotc.iso.org/livelink/livelink/open/jtc1sc27 by 2019-10-04.**
Secretariat's note:	***This document replaces SC 27 N19529 which has been withdrawn from both SC 27 Livelink and CIB (Committee Internal Balloting) application due to incorrect content provided in the NP Form (Form 4) and Attachment 1 to SC 27 N19529. In addition, SC 27 N19836 also provides an outline/draft document which was omitted in the originally circulated submission SC 27 N19529.***
ACTION:	**VOTE**
DUE DATE:	**2019-10-04**
DISTRIBUTION:	**P, O, L Members** **L. Rajchel, JTC 1 Secretariat** **J. Alcorta, ISO/CS (ITTF)** **A. Wolf, SC 27 Chairman** **L. Lindsay, SC 27 Vice-Chair** **E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG Convenors**
MEDIUM:	**Livelink server http://isotc.iso.org/livelink/livelink/open/jtc1sc27**
NO. OF PAGES:	**1 + 8 + 28 (Attachment 1)**

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Saatwinkler Damm 42/43, D-13627 [D-10772] Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-4-2652; E-mail: krystyna.passia@din.de;
HTTP://www.din.de/go/jtc1sc27

Form 4: New Work Item Proposal

Circulation date: **2019-07-12** **Closing date for voting:** **2019-10-04**	**Reference number:** **ISO/IEC NP TS 24462** (to be given by Central Secretariat) **ISO/IEC JTC 1/SC 27** **N 19836*** REPLACES N19529 **** This document replaces SC 27 N19529 which has been withdrawn from both SC 27 Livelink and CIB (Committee Internal Balloting) application due to incorrect content provided in the NP Form (Form 4) and Attachment 1 to SC 27 N19529. In addition, SC 27 N19836 also provides the outline/draft document which was omitted in the originally circulated submission SC 27 N19529.***
Proposer (e.g. ISO member body or A liaison organization) **ISO/IEC JTC 1/SC 27**	
Secretariat **DIN**	

A proposal for a new work item within the scope of an existing committee shall be submitted to the secretariat of that committee with a copy to the Central Secretariat and, in the case of a subcommittee, a copy to the secretariat of the parent technical committee. Proposals not within the scope of an existing committee shall be submitted to the secretariat of the ISO Technical Management Board.

The proposer of a new work item may be a member body of ISO, the secretariat itself, another technical committee or subcommittee, an organization in liaison, the Technical Management Board or one of the advisory groups, or the Secretary-General.

The proposal will be circulated to the P-members of the technical committee or subcommittee for voting, and to the O-members for information.

☒ The proposer has considered the guidance given in the Annex C during the preparation of the NWIP.

Proposal (to be completed by the proposer)

Title of the proposed deliverable.

English title:

Information security – Security techniques – Ontology for ICT Trustworthiness Assessment

French title:

(In the case of an amendment, revision or a new part of an existing document, show the reference number and current title)

Scope of the proposed deliverable.

We consider ICT trustworthiness assessment as a subject associated with various types of best practices and assessments, such as governance, secure development lifecycle, security evaluation, risk assessment. **The proposed Technical Specification defines an inventory of building blocks conceptually associated with different types of assessments, an ontology (i.e., a meta-model) that organizes the building blocks, and guidelines for using the inventory of building blocks and the ontology.**

Relevant areas include assessments related to governance, risk management, security evaluation, Secure Development Lifecycle (SDL), supply chain integrity, privacy, etc.

The ontology will cover the domain of ICT trustworthiness assessment and define a consistent view in this space. It will not edit or propose to edit existing standards in this area.

Formalizing the types, categories, and structural characteristics of building blocks in the area of trustworthiness assessment will increase efficiency and improve harmonization in standards development and their use.

Building blocks can refer to structural components as well as semantic components. These components can be related to a variety of concepts and activities related to trustworthiness assessments, including process related, such as traceability or elements of assessment methodologies.

For the purposes of this document, we use the following provisional terms and definitions.

Trustworthiness
Demonstrable likelihood that the system performs according to designed behavior under a typical set of conditions as evidenced by its characteristics, such as safety, security, privacy, reliability and resilience (from NIST CPS Framework v1.0).

Trustworthiness assessment
Techniques, mechanisms, and approaches used to evaluate trustworthiness of a system, environment, organization, technology or products. The approaches include, but are not limited to risk analysis, SDL (Secure Development Lifecycle), governance, deterministic testing, and other.

Building block
A component that fits with others to form a whole.

Ontology
A set of concepts and categories in a subject area or domain that shows their properties and the relations between them (Oxford Dictionary). In computer science, an ontology is associated with a standardized format that facilitates exchange of information.

Individual
The basic, "ground level" components of an ontology. The individuals in an ontology may include concrete objects such as people, animals, tables, automobiles, molecules, and planets, as well as abstract individuals such as numbers and words (although there are differences of opinion as to whether numbers and words are classes or individuals). (Wikipedia)

Class
A collection of individuals of an ontology.

Subclass
A subset of a class.

Property
An attribute describing how individuals of an ontology are related to other individuals or classes.

Purpose and justification of the proposal

The purpose of this proposal is to provide a consistent view of the ICT trustworthiness assessment space by creating a meta-model that defines structural and semantic building blocks and organizes them in an ontology. This meta-model will provide a formal view for those who administer, those who plan, and those who use assessments to understand and streamline their activities, thus improving efficiency and adoption of various types of assessments and assessment frameworks.

Background: In the past two decades, a significant body of knowledge has been developed with regard to standards relevant to different types of trustworthiness assessments and diverse assessment techniques. Work was done in such areas as evaluation criteria for IT security, testing methodologies, architectural and design principles, impact assessment, privacy assessments, SDL for various classes of systems, and many more areas.

The body of knowledge created in ICT trustworthiness assessment is extremely valuable, but it is of a considerable size. The standards in this area are connected to each other, reference each other, and are used in adjacent environments. They have similar structural and semantic elements.

Market need: the size and diversity of the trustworthiness assessment related space negatively affects the efficient operations of this area and may constitute an obstacle to faster adoption. Due to the size of the body of knowledge associated with different types of assessments, a model of structural and semantic elements (an ontology) is expected to foster a consistent view across different areas of trustworthiness related assessments, contribute to an increased adoption rate of assessment-related standards, and potentially achieve a greater degree of harmonization. It is proposed to build this model by creating an inventory of structural and semantic building blocks conceptually associated with different types of assessments and organizing the inventory in an ontology.

Problems this proposal solves: at this time, no meta-model of the trustworthiness assessment space exists, making it more difficult to obtain a consistent view of this area. The proposed technical specification is expected to create such a meta-model. In addition to the benefits already mentioned, product and technology developers are expected to be able to increase awareness of their assessment options and have a better understanding of relevant assessment components. The meta-model will allow them to make planning more efficient. Governments may be able to improve understanding of broadly applicable ICT assessment schemes for different environments, objectives, market segments, and context. As a result of the availability of the meta-model, the number of assessed technologies
may increase, and there may be better premises for the participation of SMEs and non-profit organizations in various assessment schemes.

The proposed technical specification is expected to enhance the value and visibility of the trustworthiness assessment standards to end users and thus increase their adoption.

In addition to the descriptive content and diagrams, we propose to define the building blocks in XML and to define the ontology in OWL. Availability in machine-readable formats is expected to support the inclusion of this model in various decision-support, planning, and requirements-related tools, an option that may promote the use of trustworthiness assessment standards.

To summarize, various benefits are expected to be derived from a standard meta-model of the trustworthiness assessment space, e.g.:
• Obtaining a comprehensive view of the ICT trustworthiness assessment approaches;
• Building new assessment standards faster, using existing building blocks;
• Analyzing the assessment space for gaps, similarities, and conflicts across different ICT domains;
• Increasing harmonization of the trustworthiness assessment domain;
• Improving adoption, including among SME;
• Improving product and technology planning;
• Supporting extensibility and direct incorporation into tools.

Consider the following: Is there a verified market need for the proposal? What problem does this standard solve? What value will the document bring to end-users? See Annex C of the ISO/IEC Directives part 1 for more information. See the following guidance on justification statements on ISO Connect:
https://connect.iso.org/pages/viewpage.action?pageId=27590861

Please select any UN Sustainable Development Goals (SDGs) that this deliverable will support. For more information on SDGs, please visit our website at www.iso.org/SDGs.

Goal 9: Industry, Innovation, and Infrastructure

Preparatory work (at a minimum an outline should be included with the proposal)

☐ A draft is attached ☒ An outline is attached ☐ An existing document to serve as initial basis

The proposer or the proposer's organization is prepared to undertake the preparatory work required:

☒ Yes ☐ No

If a draft is attached to this proposal:

Please select from one of the following options (note that if no option is selected, the default will be the first option):

☒ Draft document will be registered as new project in the committee's work programme (stage 20.00)
☐ Draft document can be registered as a Working Draft (WD – stage 20.20)
☐ Draft document can be registered as a Committee Draft (CD – stage 30.00)
☐ Draft document can be registered as a Draft International Standard (DIS – stage 40.00)

If the attached document is copyrighted or includes copyrighted content:

☐ The proposer confirms that appropriate permissions have been granted in writing for ISO or IEC to use that copyrighted content.

Is this a Management Systems Standard (MSS)?

☐ Yes ☒ No

NOTE: if Yes, the NWIP along with the Justification study (see Annex SL of the Consolidated ISO Supplement) must be sent to the MSS Task Force secretariat (tmb@iso.org) for approval before the NWIP ballot can be launched.

Indication(s) of the preferred type to be produced under the proposal.

☐ International Standard ☒ Technical Specification

☐ Publicly Available Specification

Proposed development track

☐ 18 months* ☐ 24 months ☒ 36 months ☐ 48 months

Note: Good project management is essential to meeting deadlines. A committee may be granted only one extension of up to 9 months for the total project duration (to be approved by the ISO/TMB).

***DIS ballot must be successfully completed within 13 months of the project's registration in order to be elligible for the direct publication process**

Draft project plan (as discussed with committee leadership)

Proposed date for first meeting: 2019-10-15

Dates for key milestones: DIS submission 2021-10-15

Publication 2022-10-15

Known patented items (see ISO/IEC Directives, Part 1 for important guidance)

☐ Yes ☒ No

If "Yes", provide full information as annex.

Co-ordination of work: To the best of your knowledge, has this or a similar proposal been submitted to another standards development organization?

☐ Yes ☒ No

If “Yes”, please specify which one(s):

A statement from the proposer as to how the proposed work may relate to or impact on existing work, especially existing ISO and IEC deliverables.
The proposer should explain how the work differs from apparently similar work, or explain how duplication and conflict will be minimized.

We are not aware of duplication. The proposed technical specification will not impact existing work and work in progress. It is complementary to these efforts.

A listing of relevant existing documents at the international, regional and national levels.

ISO/IEC TR 20943-6:2013 Information technology — Procedures for achieving metadata registry content consistency — Part 6: Framework for generating ontologies
ISO/IEC 1325 – Topic Maps
ISO/IEC CD 21838 - Information technology -- Top-level ontologies
RDF (Resource Description Framework) Specification v. 1.1 – Feb 2014, W3C OWL (Web Ontology Language) specification v.2 – Dec 2012, W3C

Please fill out the relevant parts of the table below to identify relevant affected stakeholder categories and how they will each benefit from or be impacted by the proposed deliverable(s).

	Benefits/impacts	**Examples of organizations / companies to be contacted**
Industry and commerce - large industry	-- Improved ability to define assessment requirements -- Improved ability to target assessments quickly to emerging or complex technology environments -- Improved ability to analyze assessment needs -- Access to the inventory of structural and semantic components used in different assessments -- Increased harmonization -- Decreased effort needed to collect best practices for new technology and standardization areas -- Shorter assessment times -- Decreased assessment costs -- Greater connection between product development and assessments	IBM Lenovo Infineon Amazon Alibaba GE SAP Samsung Embraer Other
Industry and commerce -- SMEs	-- Potentially improved ability to plan assessments -- Better ability to understand assessment requirements -- Less expensive assessments -- Greater ability to participate in various assessment schemes due to better visibility.	Guardtime Green Hills

	-- Most of the items applied to industry and commerce above	
Government	-- Better ability to analyze existing assessment schemes, including gap analysis -- Improved ability to anticipate assessment and certification needs -- Better ability to harmonize national and international requirements -- Better ability to provide more flexible assessment schemes for different contexts of use.	All countries that pursue assessments and certifications: China, France, Germany, UK, US, Canada, Australia, Malaysia, and others
Consumers	-- Increased trust in ICT products and services -- In the future, greater harmonization of features in ICT products and services -- Greater understanding of assessment requirements and results	
Labour	Same as Consumers	
Academic and research bodies	-- Increased research interest in standardization -- Increased participation in standardization -- Developing new models for designing and using assessments -- Developing Open Source automation tools	
Standards application businesses		
Non-governmental organizations		
Other (please specify)		

Liaisons: A listing of relevant external international organizations or internal parties (other ISO and/or IEC committees) to be engaged as liaisons in the development of the deliverable(s).	Joint/parallel work: Possible joint/parallel work with: ☐ IEC (please specify committee ID) ☐ CEN (please specify committee ID) ☐ Other (please specify)
A listing of relevant countries which are not already P-members of the committee. Not Applicable Note: The committee secretary shall distribute this NWIP to the countries listed above to see if they wish to participate in this work	
Proposed Project Leader (name and e-mail address) Sun Yan (sunyan@cesi.cn) Claire Vishik (claire.vishik@intel.com) Marcello Balduccini (mbalducc@sju.edu)	Name of the Proposer (include contact information) Sun Yan (sunyan@cesi.cn) Claire Vishik (claire.vishik@intel.com) Marcello Balduccini (mbalducc@sju.edu)
This proposal will be developed by: ☒ An existing Working Group: ISO/IEC JTC 1/SC 27/WG 3 ☐ A new Working Group: (Note: establishment of a new WG must be approved by committee resolution) ☐ The TC/SC directly ☐ To be determined:	
Supplementary information relating to the proposal ☒ This proposal relates to a new ISO document ☐ This proposal relates to the adoption as an active project of an item currently registered as a Preliminary Work Item ☐ This proposal relates to the re-establishment of a cancelled project as an active project Other:	
Maintenance agencies and registration authorities ☐ This proposal requires the service of a maintenance agency. If yes, please identify the potential candidate: ☐ This proposal requires the service of a registration authority. If yes, please identify the potential candidate: NOTE: Selection and appointment of the MA or RA is subject to the procedure outlined in the ISO/IEC Directives, Annex G and Annex H, and the RA policy in the ISO Supplement, Annex SN.	
☒ **Annex(es) are included with this proposal (give details)** Detailed outline of the proposed document as contained in Attachment 1 to .	
Additional information/question(s)	