ISO/IEC JTC 1 N 9482 2009-01-20

ISO/IEC JTC 1
Information Technology

Document Type:	**Proposed NP**
Document Title:	**SC 27 Proposal for a new work item on guidelines for security of outsourcing**
Document Source:	**SC 27 Secretariat**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for concurrent review. If the JTC 1 Secretariat receives no objections to this proposal by the due date indicated, we will so inform the SC 27 Secretariat.**
Action ID:	**ACT**
Due Date:	**2009-04-20**
No. of Pages:	**11**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	proposed NP
TITLE:	**Proposal for a new work item on Guidelines for security of outsourcing**
SOURCE:	Secretariat of JTC 1/SC 27
DATE:	2009-01-14
PROJECT:	
STATUS:	In accordance with resolution 3 (contained in SC 27 N6904) of the 5th SC 27/WG 4 meeting held in Limassol, Cyprus, 6-10 October 2008, this document is being circulated to the SC 27 National Bodies for a 3-month NWI 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 ISO e-balloting application by **2009-04-14.**
ACTION ID:	LB
DUE DATE:	**2008-01-14**
DISTRIBUTION:	P- and L-Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice-Chair E. J. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners
MEDIUM:	Livelink-server
NO. OF PAGES:	1 + 9

New Work Item Proposal

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2008-10-08	Proposer: ISO/IEC JTC 1 SC 27
Secretariat: ISO/IEC JTC 1/SC27 DIN, Germany	**ISO/IEC JTC 1/SC 27 N7221**

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal

Title: Information technology – Security techniques – Guidelines for security of outsourcing

Scope:

This International Standard will define guidance to organizations on the evaluation of security risks involved in the procurement and use of outsourced services. This standard will support the implementation of ISO/IEC 27001/27002 controls for outsourcing and should include the following areas:

- Strategic goals, objectives and business needs
- Risks and mitigation techniques
- Assurance provision

Note: It is the intent of this standard that outsourcing is not limited to ICT outsourcing, but could include other forms of outsourcing (e.g. human resources, facilities management) that have information security implications.

Purpose and justification:

In recent years, many organizations have embraced outsourcing of information technology (IT) and back-office operation services as one of the means to improve operation efficiency and reduce the total cost of IT and business operations (McDougall, 2002a, 2002b). This change has required organizations to increase their reliance on external providers for services and operations, and created an extended trust environment that the business units are increasingly depended upon to meet their goals. Such a change has also been supported by a number of regulators, in which new security requirements for compliance have been stipulated (Bank of Thailand, 2003; Matsushima, 2000; Yakcop, 2000).

In most cases, organizations have adopted ISO/IEC 27001 and ISO/IEC 27002 as their security management system and baseline for gaining the required security assurance of the outsourcing service providers (OSP), and also in ensuring adequate security risk management of such an arrangement. In ISO/IEC 27002, the required security controls relating to outsourcing service providers, known collectively as External Parties, is addressed in Sections 6.2 (External Parties), and Section 10.2 (Third party service delivery management). It is however uncertain whether these controls are sufficient and adequate to address the security of outsourcing comprehensively, from a risk management perspective. In particular, when multiple outsourcing services providers are involved, and when organizations need to change the providers during or at the end of a contractual period.

On the other hand, many organizations have also been managing the security and risk of outsourcing services effectively. Many OSPs have also claimed effective practices of security risk management of their customers' information security needs. It will be useful to have such experiences and knowledge shared as best practices to more organizations across different industries.

Programme of work

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?
_X__ a single International Standard
____ more than one International Standard (expected number: ....)
____ a multi-part International Standard consisting of .... parts
____ an amendment or amendments to the following International Standard(s) ....
____ a technical report , type ....

And which standard development track is recommended for the approved new work item?

_X_a. Default Timeframe

___b. Accelerated Timeframe

___c. Extended Timeframe

Relevant documents to be considered

Co-operation and liaison

Liaisons will be established with appropriate organizations such as the RAISE Forum.

Preparatory work offered with target date(s)

Target dates

WD 2009-07 CD 2010-07 FDIS 2011-12 IS 2012-06

Signature: ISO/IEC JTC 1/SC 27 Secretary

Will the service of a maintenance agency or registration authority be required: No
- If yes, have you identified a potential candidate?
- If yes, indicate name

Are there any known requirements for coding? No

-If yes, please specify on a separate page

Does the proposed standard concern known patented items? No
- If yes, please provide full information in an annex

Are there any known accessibility requirements and or dependencies (see: http://www.jtc1access.org)? No
- If yes, please specify on a separate page

Are there any known requirements for cultural and linguistic adaptability? No
- If yes, please specify on a separate page

Comments and recommendations of the JTC 1 or SC27- attach a separate page as an annex, if necessary

Comments with respect to the proposal in general, and recommendations thereon:
It is proposed to assign this new item to JTC 1/SC 27

Voting on the proposal - Each P-member of the ISO/IEC/JTC 1/SC 27 has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

Date of circulation: 2009-01-14	**Closing date for voting:** 2009-04-14	**Signature of Secretary:** Krystyna Passia Secretariat JTC 1/SC27

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA

Criterion	**Validity**	**Explanation**
A. Business Requirement		
A.1 Market Requirement	Essential _X_ Desirable ____ Supportive ___	There is a generally accepted need for guidelines to securely facilitate outsourcing. The proposed standard also supports users of ISO/IEC 27001 and ISO/IEC 27002 by providing additional guidance in this area.
A.2 Regulatory Context	Essential ___ Desirable ___ Supportive _X_ Not Relevant __	This standard supports regulatory needs with respect to compliance.
B. Related Work		
B.1 Completion/Maintenance of current standards	Yes ___ No _X_	This is a new area of international standardization.
B.2 Commitment to other organization	Yes ___ No _X_	
B.3 Other Source of standards	Yes ___ No _X_	Other organizations do work relevant to some of the aspects of this proposal. Liaison will be established with those that meet ISO/IEC criteria for liaison organizations. However, there is no known source of standards similar to the proposed standard.
C. Technical Status		
C.1 Mature Technology	Yes _X_ No ___	The concepts associated with this standard are mature. However, the standard will not be standardizing any particular technology; i.e. it is technology neutral.
C.2 Prospective Technology	Yes ___ No _X_	The proposed standard is technology neutral.
C.3 Models/Tools	Yes ___ No _X_	
D. Conformity Assessment and Interoperability		
D.1 Conformity Assessment	Yes ___ No _X_	The proposed standard will not mandate the use of particular methods or tools for specific purposes, so conformity assessment is not appropriate.

D.2 Interoperability	Yes ___ No _X_	
E. Adaptability to Culture, Language, Human Functioning and Context of Use		
E1. Cultural and Linguistic Adaptability	Yes _X_ No ___	The proposed standard will be internationally applicable and will not include requirements that limit its applicability in any cultural or linguistic context.
E.2 Adaptability to Human Functioning and Context of Use	Yes ___ No _X_	The proposed standard will be able to be used by the intended target audience without the need for special provisions for diverse human functioning and diverse contexts of use.
F. Other Justification	Nil	

Notes to Proforma

A. Business Relevance. That which identifies market place relevance in terms of what problem is being solved and or need being addressed.

A.1 Market Requirement. When submitting a NP, the proposer shall identify the nature of the Market Requirement, assessing the extent to which it is essential, desirable or merely supportive of some other project.

A.2 Technical Regulation. If a Regulatory requirement is deemed to exist - e.g. for an area of public concern e.g. Information Security, Data protection, potentially leading to regulatory/public interest action based on the use of this voluntary international standard - the proposer shall identify this here.

B. Related Work. Aspects of the relationship of this NP to other areas of standardisation work shall be identified in this section.

B.1 Competition/Maintenance. If this NP is concerned with completing or maintaining existing standards, those concerned shall be identified here.

B.2 External Commitment. Groups, bodies, or for a external to JTC 1 to which a commitment has been made by JTC for Co-operation and or collaboration on this NP shall be identified here.

B.3 External Std/Specification. If other activities creating standards or specifications in this topic area are known to exist or be planned, and which might be available to JTC 1 as PAS, they shall be identified here.

C. Technical Status. The proposer shall indicate here an assessment of the extent to which the proposed standard is supported by current technology.

C.1 Mature Technology. Indicate here the extent to which the technology is reasonably stable and ripe for standardisation.

C.2 Prospective Technology. If the NP is anticipatory in nature based on expected or forecasted need, this shall be indicated here.

C.3 Models/Tools. If the NP relates to the creation of supportive reference models or tools, this shall be indicated here.

D. Conformity Assessment and Interoperability

D.1 Indicate here if Conformity Assessment is relevant to your project. If so, indicate how it is addressed in your project plan.

D.2 Indicate here if Interoperability is relevant to your project. If so, indicate how it is addressed in your project plan

E. Adaptability to Culture, Language, Human Functioning and Context of Use

NOTE: The following criteria do not mandate any feature for adaptability to culture, language, human functioning or context of use. The following criteria require that if any features are provided for adapting to culture, language, human functioning or context of use by the new Work Item proposal, then the proposer is required to identify these features.

E.1 Cultural and Linguistic Adaptability. Indicate here if cultural and natural language adaptability is applicable to your project. If so, indicate how it is addressed in your project plan. ISO/IEC TR 19764 (Guidelines, methodology, and reference criteria for cultural and linguistic adaptability in information technology products) now defines it in a simplified way:

“ability for a product, while keeping its portability and interoperability properties, to:

- be internationalized, that is, be adapted to the special characteristics of natural languages and the commonly accepted rules for their se, or of cultures in a given geographical region;

- take into account the usual needs of any category of users, with the exception of specific needs related to physical constraints”

Examples of characteristics of natural languages are: national characters and associated elements (such as hyphens, dashes, and punctuation marks), writing systems, correct transformation of characters, dates and measures, sorting and searching rules, coding of national entities (such as country and currency codes), presentation of telephone numbers and keyboard layouts. Related terms are localization, jurisdiction and multilingualism.

E.2 Adaptability to Human Functioning and Context of Use. Indicate here whether the proposed standard takes into account diverse human functioning and diverse contexts of use. If so, indicate how it is addressed in your project plan.

NOTE:

1. Human functioning is defined by the World Health Organization at **http://www3.who.int/icf/beginners/bg.pdf as:**
   <<In ICF (International Classification of Functioning, Disability and Health), the term functioning refers to all body functions, activities and participation.>>

2. 2. Content of use is defined in ISO 9241-11:1998 (Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability) as: <<Users, tasks, equipment (hardware, software and materials), and the physical and societal environments in which a product is used.>>

3. 3. Guidance for Standard Developers to address the needs of older persons and persons with disabilities).

F. Other Justification Any other aspects of background information justifying this NP shall be indicated here