ISO/IEC JTC 1 N 9047

2008-05-06

ISO/IEC JTC 1
Information Technology

Document Type:	**Proposed NP**
Document Title:	**SC 27 New Work Item Proposal on Guidance for auditors on ISMS controls**
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:	**2008-08-06**
No. of Pages:	**5**

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC 1/SC 27 N6621rev1

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	text for NP ballot
TITLE:	New Work Item Proposal on Guidance for auditors on ISMS controls
SOURCE:	Secretariat of JTC 1/SC 27
DATE:	2008-05-05
PROJECT:	**NWIP**
STATUS:	In accordance with resolution 24 (see SC 27 N6799) of the 20th SC 27 Plenary meeting held in Kyoto, 2008-04-21/22 , this document is circulated to the SC 27 National Bodies for a 3-month NP letter ballot and to JTC 1 for a concurrent review. P-Members of SC 27 are requested to submit their votes on the above-mentioned NWI Proposal via the ISO e-balloting application by **2008-08-05.**
ACTION ID:	**LB**
DUE DATE:	**2008-08-05**
DISTRIBUTION:	P-, O- 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 + 3

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

New Work Item Proposal

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2008-04-18	Proposer: SC 27
Secretariat: ISO/IEC JTC 1/SC 27	**ISO/IEC JTC 1 N** XXXX ISO/IEC JTC 1/SC 27 N6621rev1

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: Guidance for auditors on ISMS controls

Scope:

This Technical Report provides guidance for all auditors regarding ISMS controls selected through a risk-based approach (e. g. as presented in a statement of applicability) for information security management. This Technical Report supports the information security risk management process and internal, external and third-party audits of an ISMS by explaining the relationship between the ISMS and its supporting controls. It provides guidance on how to verify the extent to which required ISMS controls are implemented. Furthermore, it supports any organization using ISO/IEC 27001 and ISO/IEC 27002 to satisfy assurance requirements, and as a strategic platform for Information Security Governance.

This TR is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. The TR is applicable to organizations of all sizes regardless to the extent of their reliance on information.

Purpose and justification

- To support planning and execution of ISMS audits and the Information Security Risk Management process.
- To further add value, and enhance the quality and benefit of the ISO/IEC 27000 Family to the end-user by closing the gap between reviewing the ISMS in theory and, when needed, verifying evidence of implemented ISMS controls (e.g. in the end-users organization, business processes and system environment).
- To provide guidance for auditing controls based on the guidance provided by ISO/IEC 27002.
- To improve ISMS Audits by optimizing the relationships between the ISMS processes and required controls (e.g mechanisms to limit harm caused by failures in the protection of information - erroneous financial statements, incorrect documents issued by an organization and intangibles such as reputation and image of the organization and privacy, skills and experience of people).
- To support an ISMS based assurance and Information Security Governance approach and audit thereof.
- To ensure effective and efficient use of audit resources.

Programme of work

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?
_ _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)
.....
___X_ a technical report , type 2.....

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

__**X**_ a. Default Timeframe

___ b. Accelerated Timeframe (Fast Track)

____ c. Extended Timeframe

Relevant documents to be considered

The latest edition of the referenced document (including any amendments) applies.

- ISO/IEC 27001
- ISO/IEC 27002

Co-operation and liaison

Preparatory work offered with target date(s)

The target dates are:

- PDTR November 2009
- DTR May 2011
- TR November 2011

Signature: SC 27/WG 1

Contact: Anders Carlstedt

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

Comments and recommendations of the JTC 1 or SC 27- attach a separate page as an annex, if necessary

{PRIVATE }Comments with respect to the proposal in general, and recommendations thereon:
It is proposed to assign this new item to JTC 1/SC 27 which has agreed to this assignment.

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

Date of circulation: 2008-05-08	**Closing date for voting:** 2008-08-05	**Signature of Secretary:** Krystyna Passia Secretariat of JTC 1/SC 27

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	**Validity**	**Explanation**
A. Business Requirement		
A.1 Market Requirement	Essential _**X**_ Desirable ___ Supportive ___	There is a market need for the development of guidance on ISMS ISMS controls for auditors to support the ISMS process.
A.2 Regulatory Context	Essential ___ Desirable ___ Supportive ___ Not Relevant _ **X**	
B. Related Work		
B.1 Completion/Maintenance of current standards	Yes ___ No_ **X** _	
B.2 Commitment to other organisation	Yes _ __ No__X	
B.3 Other Source of standards	Yes ___ No _ **X** _	
C. Technical Status		
C.1 Mature Technology	Yes _ **X** _ No___	
C.2 Prospective Technology	Yes __ No___	
C.3 Models/Tools	Yes ___ No___	
D. Conformity Assessment and Interoperability		
D.1 Conformity Assessment	Yes _ _ No__**X**_	
D.2 Interoperability	Yes __ No_ **X** __	
E. Cultural and Linguistic Adaptability	**Yes**__ **X** __ **No**_____	