



ISO/IEC JTC 1/SC 27 **N14177**

ISO/IEC JTC 1/SC 27/WG 5 **N514177**

REPLACES: SC 27 N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

**DOC TYPE:** Standing Document

**TITLE:** **WG5 Standing Document 5 —  
Explanation on the use of ISO/IEC 27001 (ISMS) for privacy  
management**

**SOURCE:** Editor/Co-editors (M. Reinis/M. Grall, R. Jain)

**DATE:** 2014-06-16

**PROJECT:** **WG 5 SD5**

**STATUS:** As per resolution 2 (contained in SC 27 N14199) of the 17th meeting of ISO/IEC JTC 1/SC 27/WG 5 in Hong Kong, China, 7<sup>th</sup> – 11<sup>th</sup> 2014, this document has been updated and is hereby circulated to experts, National Bodies and liaison organizations for study and comment by **2014-09-24**.

**PLEASE submit your contribution on the hereby attached document via the SC 27 e-balloting website at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>**

**PLEASE NOTE:** For comments please use the SC 27 TEMPLATE separately attached to this document.

**ACTION:** **COMM**

**DUE DATE:** **2014-09-24**

**DISTRIBUTION:** P-, O- and L-Members  
W. Fumy, SC 27 Chairman  
M. De Soete, SC 27 Vice Chair  
E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenber, WG-Convenors

**MEDIUM:** <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

**NO. OF PAGES:** 1 + 5

# **WG5 Standing Document 5 — Explanation on the use of ISO/IEC 27001 (ISMS) for privacy management**

## **1 Introduction**

This Standing Document is intended to explain the ways in which privacy management related aspects can be best addressed through ISO/IEC 27001 or ISO/IEC 27009, considering the existing standards of ISO/IEC JTC 1/SC 27 and standards under development in ISO/IEC JTC 1/SC 27.

In addition, this standing document is intended to identify the privacy related areas of ISMS that are not addressed by existing standards and those under development and to facilitate discussions on the possibility of developing a privacy management system going forward.

This Standing Document will contain in Annex A an cross reference, pointing to

- ⤴ ISO/IEC 27001 requirements, extending them with privacy specific requirements, and
- ⤴ ISO/IEC 27002 controls, considering further sets of privacy controls.

This Standing Document may also include aspects that may provide valuable inputs to the existing or new projects related to privacy to close identified gaps in the area on management of privacy.

This Standing Document is addressed to ISO/IEC JTC1 SC 27, its WGs or other organizations such as JTC1 SCs, ISO TCs and other SC 27/WG 5 Liaison organizations. It is acknowledged that the references provided here need to be continuously reviewed and maintained.

## **2 Overview**

*NOTE: This clause is intended to explain the situation, for example by presenting shortly ISO/IEC 27001, ISO/IEC 27009, what has been decided in the PIMS SP*

ISO/IEC 27001 provides requirements for an information security management system (ISMS). It also provides in its Annex A a set of generic information security controls that are used for comparison to the controls used to treat the appreciated information security risks.

ISO/IEC 27009 provides provision for creating sector specific standards that could be used in the ISO/IEC 27001 framework. "Sector" is used as the generic term to refer to everything that is not information security only. The understanding of "sector" includes privacy (or PII protection).

It has been decided during the PIMS Study Period that no privacy specific management system should be created, but to use the ISO/IEC 27001 framework to deal with privacy instead.

Thus, if there is a need for dealing with privacy management, ISO/IEC 27001 has to be taken as a basis, and ISO/IEC 27009 requirements should be fulfilled.

As an example, it is possible to refine and define additional requirements to those from ISO/IEC 27001, but such modification must never contradict, remove or invalidate any of the requirements in ISO/IEC 27001.

## **3 Relationship between Security and Privacy**

*NOTE: This clause is intended to explain the possible interactions between information security and privacy*

While key goal of Information security is to protect an organization against risks related to its information, the key privacy goal is to protect PII principals against the risks pertaining to the processing of their PII by the organizations. Even if the goals differ, the way risks are managed and management system works is very close, since PII is a specific kind of information.

Actually, the main difference is related to the impact on the privacy of PII principals, and not on the organization. Thus, there is a need for explaining that specificity, and maybe some others. But presently there is no requirement standard for that purpose. WG5 is developing privacy guidelines and sets of controls,

such as ISO/IEC 29134 for the PIA, ISO/IEC 29151 for generic privacy controls, and ISO/IEC 27018 for privacy controls for cloud services providers. They could be useful in the privacy specific application of ISO/IEC 27001.

### 3.1 Application of privacy as a sector in ISMS based on ISO/IEC 27001

S. No.	ISO 27001:2013 – Requirements	Relevant for privacy? <sup>1</sup>	Topic
1	4. Context of the organization 4.1 Understanding the organization and its context 4.2 Understanding the needs and expectations of interested parties 4.3 Determining the scope of the information security management system 4.4 Information security management system	ISO/IEC 29134  ISO/IEC 29100  ISO/IEC 29134	Privacy risk criteria  Privacy safeguarding requirements Privacy stakeholder Business process and purpose PII Flow, Privacy supporting assets
2	5. Leadership 5.1 Leadership and commitment 5.2 Policy 5.3 Organizational roles, responsibilities and authorities	ISO/IEC 29100	Privacy by Design/Default Privacy policy Data Privacy Officer Privacy risk owners
3	6. Planning  6.1 Actions to address risks and opportunities 6.2 Information security objectives and plans to achieve them	ISO/IEC 29134	Privacy impact assessment Privacy risk assessment  Privacy risk treatment
4	7. Support 7.1 Resources 7.2 Competence 7.3 Awareness 7.4 Communication  7.5 Documented information		Privacy Incident Mgmt Privacy awareness Privacy communication, transparency
5	8. Operation 8.1 Operational planning and control 8.2 Information security risk assessment 8.3 Information security risk treatment	ISO/IEC 29134	Privacy Lifecycle Mgmt Privacy risk assessments Privacy risk treatment
6	9. Performance Evaluation 9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit 9.3 Management review	ISO/IEC 29151  [ISO/IEC 29190 <sup>2</sup> ]	Privacy measurement  [Privacy capability maturity]
7	10. Improvement 10.1 Nonconformity and corrective action 10.2 Continual improvement		
8	Annex A	ISO/IEC 29151 ISO/IEC 27018	Privacy controls

**Table 1:** Mapping of ISMS requirements with privacy standards and topics

*[Editors` note: More efforts are required to fill this table and do a detailed mapping of ISMS requirements and relevant provisions of the published or under development WG5 privacy standards. Also, it needs to be*

<sup>1</sup> Whether the requirement is relevant for privacy or not; If yes, whether addressed in existing privacy standards or those under development (which ones?); If not addressed, then how can these management system requirements may be addressed? What is specific to privacy which may need refinement of existing requirements or addition of new requirements? How can this work within ISO SC27?

<sup>2</sup> ISO/IEC 29190 on Privacy capability model might not be suitable in this regard – subject for later evaluation

*analyzed whether for any ISMS requirement which is not addressed in any of the existing privacy standards, the requirement needs to be referred as it is or some customization is recommended.]*

## **4 Impact on WG5 standards**

*NOTE: This clause is intended to explain the issues regarding the use of ISO 27001 (ISMS) for privacy management, and how can these issues be addressed.*

In order to define the privacy specific requirements, in addition to those from ISO/IEC 27001, a new standard can be created. This standard will have to fulfill the ISO/IEC 27009 requirements. It could be possible to make references to the WG5 existing standards that provide provision for implementing ISO/IEC 27001 requirements.

Furthermore, additional efforts may be required to explore how privacy principles that go beyond the domain of security can be best addressed in the existing ISMS, esp. given that security is one of the privacy principles. The existing approach of mapping additional controls directly to privacy principles instead of management areas or risks (as followed in ISO/IEC 27018 and ISO/IEC 29151) may not be the best way to proceed.

If there is a need for using privacy specific sets of controls such as ISO/IEC 29151 and ISO/IEC 27018 in the ISO/IEC 27001 framework, in addition to those from ISO/IEC 27001 Annex A in an ISMS framework, those standards will have to fulfill the ISO/IEC 27009 requirements. Refer A.1 section of this document.

Guidelines such as ISO/IEC 29134 could be referred as useful material to implement some of the requirements related to risk management in the privacy specific context. Refer A.2 section of this document.

# Annex A

## Additions to consider for the protection of PII

*[Editors` note: Some of the WG5 projects referred to in this clause are pending for requests on title and/or scope. The text can only reflect the status that is currently given, not the new title or scope to be]*

### A.1 Additional requirements to ISO/IEC 27001

If an organization intends to use the International Standard ISO/IEC 27001 for the protection of personally identifiable information (PII), sometimes also referred to als „privacy“, in addition to the requirements given in ISO/IEC 27001, the following requirements apply:

#### A.1.1 Determining the scope of the information security management system

The requirements specified in clause 4.3 of ISO/IEC 27001 apply.

In addition, the organization shall consider privacy principles set in ISO/IEC 29100 and organizational self-obligations concerned with PII.

The scope shall state that the protection of PII is a dedicated objective that is intended to be achieved by the application of the information security management system.

#### A.1.2 Actions to address risks and opportunities

The requirements specified in clause 6.1 of ISO/IEC 27001 apply.

In addition, the organization shall define and apply a joint information security and privacy risk assessment process that:

- a) identifies the privacy risks related to PII;
- b) analyze the potential consequences on PII principals' privacy that would result if the risks identified were to materialize.

In addition, the organization shall define and apply a joint information security privacy risk treatment process to:

- a) compare the controls determined with the ISO/IEC 29100 privacy principles.

NOTE: ISO/IEC 29134 Privacy impact assessment - Methodology provides further guidance for the assessment and the treatment of the privacy risks related to PII.

Title: ISO/IEC 29134 Privacy impact assessment - Methodology

Scope: This International Standard:

- ▲ gives guidelines for a process for the conducting of privacy impact assessments;
- ▲ describes a structure and content of a PIA report.

It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations.

This International Standard is relevant to those involved in designing or implementing projects, including operating data processing systems and services, that use PII that may have an impact on privacy within an organization and, where appropriate, external parties are supporting such activities.  
[Editorial note: This scope that is intended to be approved on an upcoming request for a scope change]

Status: by spring 2014, this project is on 3<sup>rd</sup> WD stage

Sector: This International Standard is relevant to the application of any ISMS with the cross functional requirement to protect personally identifiable information (PII), sometimes also referred to as „privacy“.

## **A.2 Additional controls to ISO/IEC 27002**

If an organization intends to use the International Standard ISO/IEC 27001 for the protection of personally identifiable information (PII), in addition to the controls given in ISO/IEC 27002, the following sets of normative controls apply with respect to the dedicated scope of the document:

### **A.2.1 Code of practice for PII protection**

Title: ISO/IEC 29151 Code of practice for PII protection

Scope: This International Standard establishes commonly accepted control objectives, controls and guidelines for implementing controls, which are usable for the treatment of risks that have been generated on PII principals and previously assessed, for example, by a PIA when processing of PII by an organization.

In particular, this International Standard specifies guidelines based on ISO/IEC 27002 in accordance with the privacy principles in ISO/IEC 29100, taking into consideration the regulatory requirements for processing PII 8 which may be applicable within the context of an organization's information security risk environment(s) as well as privacy controls.

This International Standard is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, such as PII controllers that collect personally identifiable information and determine the purposes for which it is processed, and PII processors that process personally identifiable information on behalf of the PII controller.

Status: by spring 2014, this project is on 2<sup>nd</sup> WD stage

Sector: This International Standard is relevant to the application of any ISMS with the cross functional requirement to protect personally identifiable information (PII), sometimes also referred to as „privacy“.

### **A.2.2 Code of practice for PII protection in public cloud acting as PII processors**

Title: ISO/IEC 27018 Code of practice for PII protection in public cloud acting as PII processors

Scope: This International Standard establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

In particular, this International Standard specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of Personally Identifiable Information which may be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

This International Standard is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations.

The guidelines in this International Standard may also be relevant to organizations acting as PII controllers; however, PII controllers may be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. This International Standard is not intended to cover such additional obligations.

Status: by spring 2014, this project is at DIS stage

Sector: This International Standard is relevant to organizations acting as an operator in the area of public cloud business.