INTERNATIONAL STANDARD

ISO/IEC 29190

First edition
2015-08-15

Information technology — Security techniques — Privacy capability assessment model

Technologies de l'information — Techniques de sécurité — Modèle d'évaluation de l'aptitude à la confidentialité

Reference number
ISO/IEC 29190:2015(E)

© ISO/IEC 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Methodology **1**
4.1 Introduction 1
4.2 Define a privacy capability assessment model 2
4.3 Capability scale 4
4.4 Rate the process's current capability vs. target capability 5
4.5 Determine sub-optimal processes 6
4.6 Identify proposals for changing processes 6
4.7 Modify processes 7
5 Capability assessment process **7**
5.1 Introduction 7
5.2 Plan the assessment 7
5.3 Identify privacy activities and target capabilities 8
5.4 Identify privacy-related processes 9
5.5 Prepare criteria for information collection 9
5.6 Collect and analyse information 10
5.7 Present results 11
6 Example of a business function approach **11**
Bibliography **15**

© ISO/IEC 2015 – All rights reserved

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *Security techniques*.

© ISO/IEC 2015 – All rights reserved

Introduction

The aim of this International Standard is to provide organizations with high-level guidance about how to assess the level of their ability (capability) to manage privacy-related processes. This International Standard focuses on an approach for assessing the efficiency and effectiveness of privacy-related processes used by organizations.

Guidance on the issue of privacy management needs is multi-faceted as follows:

— The decision support information useful to a senior executive in formulating and executing a privacy strategy is different from the decision support useful to operational and line-of-business staff even though their various activities might all ultimately be directed towards the same goal;

— There are likely to be multiple "privacy stakeholders" (that is, parties who have an interest in the way the organization manages privacy). Those stakeholders might impose very different requirements, for example, driven by legal and regulatory compliance requirements, but also by inter-related "good practice" provisions stipulated, for example, by policies, codes-of-conduct, business risk assessments, audit findings, reputational, and/or financial imperatives and/or personal privacy preferences.

A broader, good practice context is important because it is possible for an organization to meet its legal and regulatory compliance obligations and still suffer significant damage if it fails to address the requirements of the other stakeholders. An assessment of the organization's capabilities in this area will need to meet the following principal sets of criteria:

— It needs to provide the organization with information which is useful to the appropriate level or levels of management;

— It needs to cater for the fact that "capability" needs to be assessed in many different domains (legal compliance, risk management, reputation, and so on).

This International Standard is aimed at those individuals responsible for directing, managing, and operating an organization's privacy management capabilities, or those responsible for advising the relevant stakeholder group. Thus, the capability model will consider multiple kinds of privacy stakeholder requirements and will result in guidance to multiple levels of stakeholders, from enterprise strategists to operational and line-of-business managers.

This International Standard provides guidance for how to set up a capability assessment program within an organization. It is expected that the management of the organization will need to apply an iterative and incremental process of improvement using the criteria defined for assessing their privacy capability. Once a baseline assessment has been identified and a set of targets for improvement of the organization's capability has been agreed, then the assessment will need to be periodically repeated in order to move the organization, over increments, towards the targeted level of capability desired by the organization.

This International Standard guides organizations towards the production of several different kinds of output:

— an overall "score" against a simple capability assessment model;

— a set of metrics indicating assessment against key performance indicators;

— the detailed outputs from privacy process management audits and management practices (for example, assessment against data protection criteria and data custody best practice) for input into improving capability in these specific areas.

© ISO/IEC 2015 – All rights reserved

Information technology — Security techniques — Privacy capability assessment model

1 Scope

This International Standard provides organizations with high-level guidance about how to assess their capability to manage privacy-related processes.

In particular, it

— specifies steps in assessing processes to determine privacy capability,

— specifies a set of levels for privacy capability assessment,

— provides guidance on the key process areas against which privacy capability can be assessed,

— provides guidance for those implementing process assessment, and

— provides guidance on how to integrate the privacy capability assessment into organizations operations.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

ISO/IEC 33001:2015, *Information technology — Process assessment — Concepts and terminology*

ISO/IEC 33020:2015, *Information technology — Process assessment — Process measurement framework for assessment of process capability*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29100 and ISO/IEC 33001 and apply.

4 Methodology

4.1 Introduction

In the current global environment, there is a tendency towards collection, use, disclosure and retention of more and more personally identifiable information (PII), for purposes ranging from support for business operations to national security and law enforcement. As is evident from the regular notification of privacy breaches, much more work is required on the part of organizations to adequately protect the PII that they are collecting, using, disclosing and retaining, as required by relevant national regulatory laws.

© ISO/IEC 2015 – All rights reserved