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 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

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*.

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.

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.

One way to develop and refine an organization's processes is to begin with an assessment of their existing capabilities in this area. To perform a process assessment in the privacy domain, typically involves the following activities:

— Define a privacy capability assessment model (see 4.2);

— Define a capability scale (see 4.3);

— Rate the process's current capability vs. target capability (see 4.4);

— Determine sub optimal processes (see 4.5);

— Identify proposals for changing processes (see 4.6);

— Modify processes (see 4.7);

— Identify the privacy activities and target capability (see 5.1);

— Identify the privacy-related processes (see 5.4);

— Prepare criteria for information collection (see 5.5);

— Collect and analyse information from privacy-related processes (5.6).

An optional additional subsequent action is to map the capability determination (i.e. the target capability level) to a scale taken from a process assessment model to assist in goal setting, comparative analysis (i.e. to measure current capability and use as a baseline for assessing an incremental process improvement target), and continual improvement strategies (i.e. develop a context or business function improvement strategy to use in planning for a process improvement project).

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

— an over-all "score" against a simple capability assessment such as the example of the six-level model described in 4.3;

— a set of metrics indicating assessment against key performance indicators in areas such as those described in the second example in 5.1;

— the detailed outputs from audit and management disciplines in specific areas of privacy management (for example, assessment against data protection criteria and data custody best practice).

4.2 Define a privacy capability assessment model

ISO/IEC 3300x is a suite of International Standards that has been developed by the ISO/IEC JTC 1/SC 7 *Software and system engineering* committee. It provides information on the concepts of process assessment and its use in process improvement and process capability determination. ISO/IEC 29190 uses the concepts of ISO/IEC 3300x for the assessment of privacy capability.

For the purposes of this International Standard, a process assessment model is related to one or more process reference models. It forms the basis for the collection of evidence and rating of a process quality characteristic. The relationships within the process assessment model is shown in Figure 1.

The information collected during assessments should be referenced against this model in order to determine a relative capability.

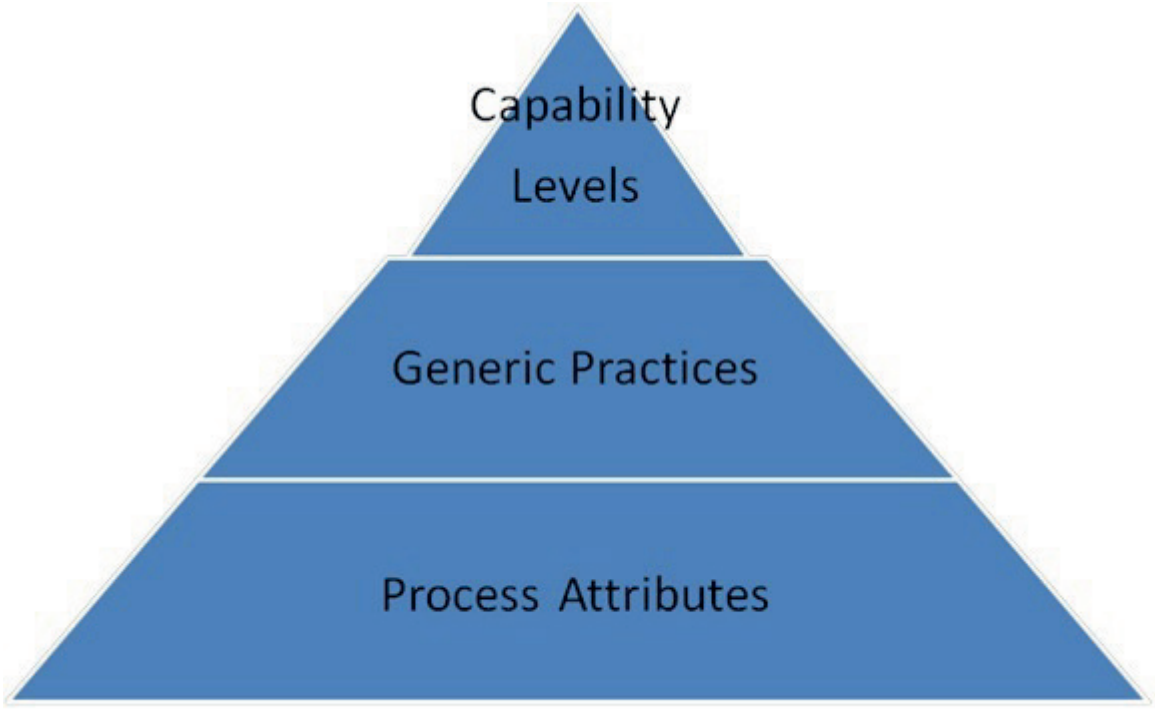

Figure 1 — Process assessment model relationships

Privacy capability assessment assumes a cycle of continuous improvement, as shown in Figure 2.

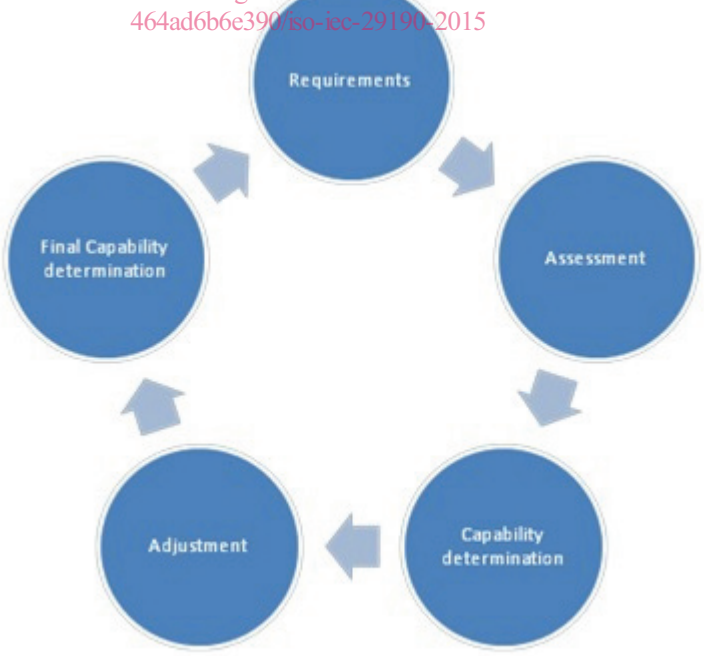

Figure 2 — Lifecycle of privacy capability assessment

With some refinement, a capability assessment model can be used to assess how competent an organization is with respect to, for instance, protecting PII as required by relevant national regulatory

laws. A capability assessment model can also be used as a benchmark for comparing different organizations where there is something that can be used as a basis for comparison. For the purposes of this International Standard, the basis for comparison should be the organizations' processes for handling PII in a manner compliant with national regulatory laws and relevant good practice.

A capability assessment model typically involves the following aspects:

a) Capability Levels: a layered framework providing a progression to the discipline needed to engage in continuous improvement. It is important to note that an organization needs to develop the ability to assess the impact of a new practice, technology or tool on their business activities. Hence it is not a matter of adopting these rather it is a matter of determining how innovative efforts influence existing practices.

   This empowers projects, teams, and organizations by giving them the foundation to support reasoned choice.

b) Key Process Areas: this identifies a cluster of related activities which, when performed collectively, achieve a set of goals considered important.

c) Goals: the goals of a key process area summarize the states that need to exist for each key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator how well the organization has established that capability level. The goals signify the scope, boundaries and intent of each key process area.

d) Common Features: common features include practices that implement and institutionalize a key process area.

   Common features are frequently defined as: Commitment to Perform; Ability to Perform; Activities Performed, Measurement and Analysis, and Verifying Implementation.

e) Key Practices: the key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the key process areas.

   The objective of this International Standard is to provide guidance to organizations on assessing how mature they are with respect to compliance with privacy and data protection legislation and relevant good practice. This International Standard focusses on assessing those activities that organizations should carry out in order to demonstrate such compliance.

4.3 Capability scale

A process assessment is a disciplined evaluation of an organizational unit's processes against a process assessment model. A processes assessment aims to determine how well the processes in the current practice are performing relative to their goals and to locate areas of weakness.

A capability assessment model needs to be a structured collection of elements that describe the characteristics of effective processes. In the form documented by ISO 33020, the model allows an organization to rate its processes on the following capability scale:

Level 0: Incomplete process

— The process is not implemented, or fails to achieve its process purpose. At this level there is little or no evidence of any systematic achievement of the process purpose.

Level 1: Performed process

— The implemented process achieves its process purpose.

Level 2: Managed process

— The performed process is implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.

Level 3: Established process

— The managed process is implemented using a defined process capable of achieving its process outcomes.

Level 4: Predictable process

— The established process operates within defined limits to achieve its process outcomes.

Level 5: Innovating process

— The predictable process is continuously improved to respond to change aligned to organizational goals.

This capability scale provides a layered framework to advance the disciplines needed to engage in continuous improvement. This empowers projects, teams, and organizations by giving them the foundation to support reasoned choice.

With profiling, the model can be used to assess an organization's capability with respect to, for instance, protecting PII as required by relevant national regulatory laws.

A capability model can also be used as a benchmark for comparing different organizations once there is a common model that can be used as a basis for comparison. For the purposes of this International Standard, the basis for comparison is the organizations' processes for handling PII in a manner compliant with national regulatory laws and relevant good practice.

There is benefit in including this capability scale, as it is of more use (to the corporate executive responsible) than some of the more detailed analysis and audit results which one could expect from assessment at the "key performance indicator" level (see Annex A).

4.4 Rate the process's current capability vs. target capability

The extent of achievement of a capability determined in accordance with 4.3 is assessed based on a four-point rating scale. In each case, the target capability against which assessments are made should be as defined in corporate privacy policies and practices:

Not achieved (0 - 15%);

— There is little or no evidence of achievement of the defined capability in the assessed process.

Partially achieved (>15% - 50%);

— There is some evidence of an approach to, and some achievement of, the defined capability in the assessed process. Some aspects of achievement of the capability may be unpredictable.

Largely achieved (>50%- 85%);

— There is evidence of a systematic approach to and significant achievement of, the defined capability in the assessed process. Some weakness related to this capability may exist in the assessed process.

Fully achieved (>85% - 100%).

— There is evidence of a complete and systematic approach to and full achievement of the defined capability in the assessed process. No significant weaknesses related to this capability exist in the assessed process.

The rating should be based upon information collected against the practice indicators, which demonstrate fulfilment of the process capabilities.