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 ..... **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**

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.

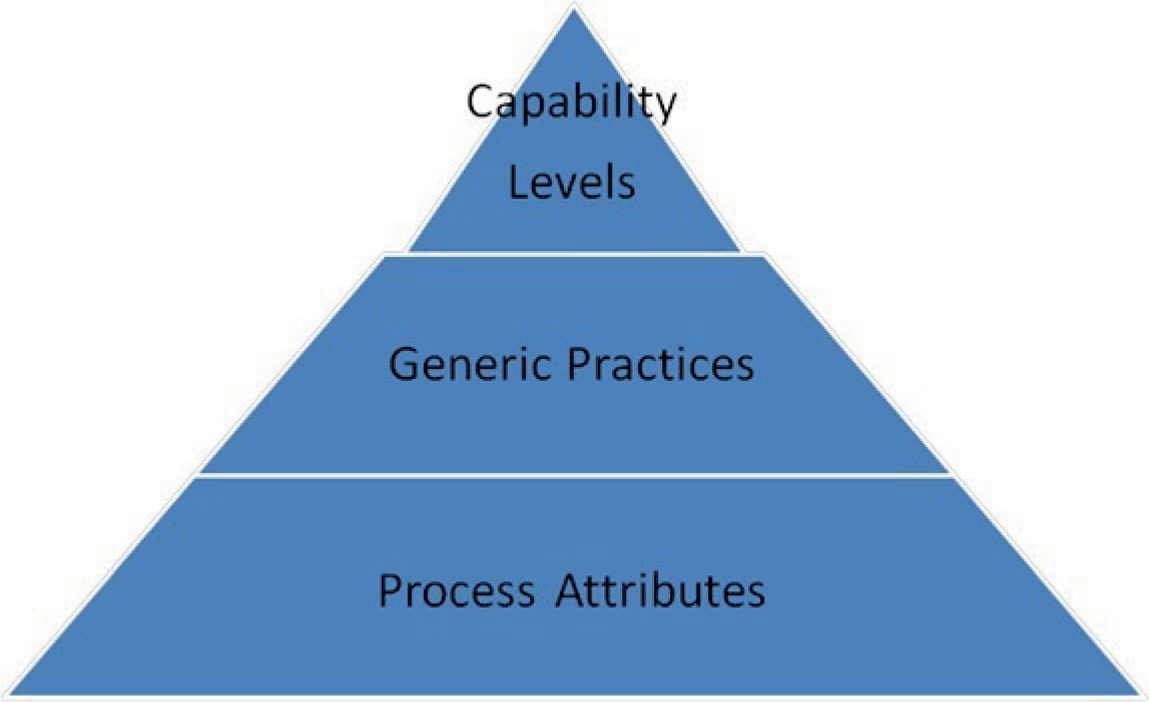

Figure 1 — Process assessment model relationships

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

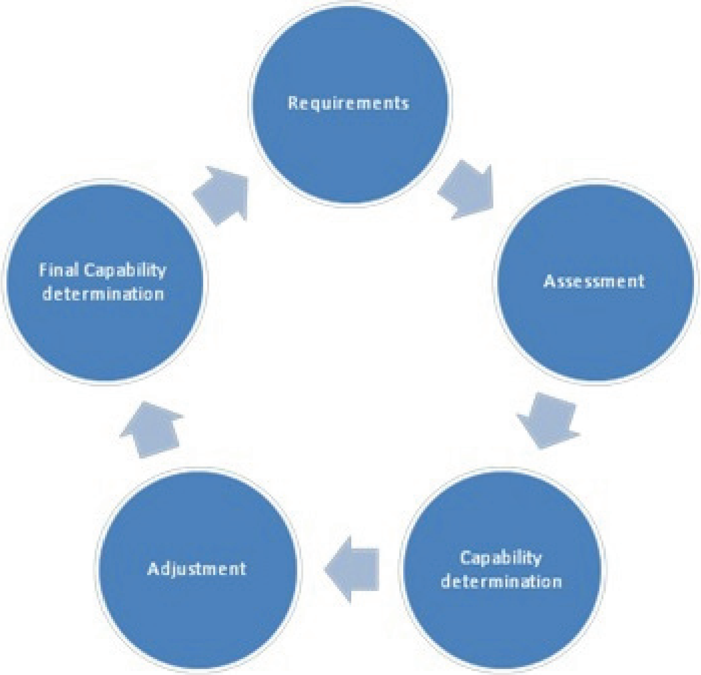

Figure 2 — Lifecycle of privacy capability assessment

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.

A rating should be identified for each of the capabilities applicable to the target privacy capability level. This should involve rating each of the capabilities that are assigned to the target privacy capability level (e.g. for 'Managed' there are:

- Process Performance;
- Performance Management;
- Work Product Management.)

This will result in not a singular rating result but rather a multi-dimensional rating result. Where a complex set of results are provided to the organization's management, it may be necessary to include explanations and descriptions of the information provided in order to ensure an appropriate level of understanding. In some circumstances, a summary report should be provided. This adds to the importance of conducting a thorough assessment planning step (see 5.1) prior to conducting the assessment.

As well as defining a suitable scope, participants and assessment team as a part of the definition of the assessment constraints for a privacy capability assessment, the sponsor and competent assessor need to agree on the types of objective evidence and the terms for each indicators to be used so that reporting of results is consistent and objective.

4.5 Determine sub-optimal processes

Sub-optimal processes (e.g. gaps) should then be identified from the existence of gaps between a target capability and an assessed capability. A gap is said to exist:

- if the target capability requires that a particular capability be Fully achieved, while the assessed capability is less than Fully achieved;
- if the target capability requires that a particular capability be Largely achieved, while the assessed capability is less than Largely achieved.

The potential consequence of a gap depends upon the capability level and process capability where the gap occurs.

The assessment should also identify specific areas of process major and minor non-conformance and other recommendations for improvement, as sources for determining sub-optimal processes. It is also important that findings in an assessment should be based on documented evidence or the lack of required evidence to support achieving target level for a business process.

4.6 Identify proposals for changing processes

The business goals of an organization in relation to privacy are often centred around:

- providing the PII principal with the capacity to perform their rights regarding their PII;
- achieving compliance with legislation and regulation.

These key management concerns become drivers that initiate process improvement throughout the organization with objectives of:

- improving the processing of PII;
- ensuring the transparency of processing of PII;
- decreasing development and maintenance costs of systems that manage PII;
- reducing the risk of breaches of privacy;
- improving the processes for dealing with privacy breaches.

From an analysis of the organization's business goals and existing stimuli for improvement, the objectives of process improvement are set. These objectives should be used to identify which sub-optimal processes identified in 4.5 needs to be selected for modification.

4.7 Modify processes

The modification of the sub-optimal processes should be implemented as a project in its own right, with defined sponsorship, project management, budget, milestones and accountability. In short, the project should be managed according to a project management process, aligned to the Process Assessment Model being used.

The objectives of the modifications should be to improve the capability based on the existing capabilities.

5 Capability assessment process

5.1 Introduction

This section describes the process of assessing the capability of an organization or process to manage their privacy-related processes. The process consists of the following steps:

— plan the assessment;

— identify privacy activities and target capabilities;

— identify privacy-related processes;

— prepare criteria for information collection;

— collect and analyse information;

— present results.

5.2 Plan the assessment

The first stage in carrying out a process capability assessment is the planning of the assessment. This typically involves a number of steps:

— identify the target of the assessment;

— identify the purpose and objectives for the assessment, including the level of capability required;

— identify a project sponsor and a lead assessor and define their roles;

— determine the approach (for example that given in this International Standard);

— determine whether other International Standards (such as ISO/IEC 9000) are relevant to the assessment;

— determine the assessment deliverables (such as a status report, a list of sub-optimal processes and/or proposals for process modification);

— identify and train the assessment team (to include the relevant process owners);

— communicate purpose and plan to those to be assessed;

— schedule and run the assessment interviews;

— agree an assessment timetable.

5.3 Identify privacy activities and target capabilities

This process is a cluster of related activities which, when performed collectively, identify a set of privacy-related procedures. This process offers a focus for applying target capabilities that need to be implemented in an effective and lasting manner. The extent to which this process has been accomplished is an indicator of how much capability the organization has established at each capability level. This also signifies the scope, boundaries and intent of each privacy-related process.

There are numerous approaches to assembling these processes and it is outside of the scope of this International Standard to prescribe a single approach. However, to help readers to better understand this requirement, two examples of possible approaches are shown below:

First example, a context approach:

- conceptual framework;
- legal context;
- implementation readiness;
- process readiness;
- regulatory and compliance criteria;
- adoption culture/behaviour.

Second example, a business function approach:

- **Inventory** – identification of business lines, supports functions dealing with PII processing, drawing up of an inventory of the corresponding processing of PII (how the PII is processed, accessed and transmitted);
- **Legal Analysis** — definition of the organization's liability (PII controller vs. PII processor) for each processing of PII and the legal requirement applicable; feed and use of the legal monitoring and intelligence to implement regulatory evolutions;
- **Policy** — the existence of binding and enforceable written privacy policies and procedures that reflect applicable laws, regulations and industry standards;
- **Executive Oversight and Governance** — internal executive oversight and responsibility for privacy and the protection of PII at the corporate and business unit levels;
- **Allocation of Staffing Resources** — allocation of resources to ensure that the organization's privacy programme is adequately staffed by adequately trained personnel. Define the hierarchical and functional structure of the organization, positioning of IT/security organization, legal/compliance services and map their roles and relationships regarding privacy management. Assign roles and responsibilities;
- **Reporting and Information Flows** — coordination and collaboration for privacy, implementing appropriate consultation and communication network and tools, steering committee, privacy communication forums, etc.;
- **Education and Awareness** — existence of up-to-date education and awareness programmes to keep employees and contractors aware of privacy policies and procedures;
- **Risk Management** — implementation of processes to assist the organization in understanding the risks to privacy raised by new products, services, technologies and business models, and to treat those risks. Periodic review of the totality of the programme to determine whether modification is necessary;
- **Claims and Complaint Handling** — procedures for responding to inquiries and complaints. Implementation of the right of the PII principals through transparency towards PII principals;

- **Compliance and Internal Enforcement** — internal enforcement of the organization’s policies and discipline for non-compliance;
- **Data Breach Management** — method by which an organization provides remedies for those whose privacy has been put at risk.

5.4 Identify privacy-related processes

The processes discussed in 5.1 should encapsulate the infrastructure, processes and procedures designed to contribute to the implementation and institutionalization of the privacy-related operational goals.

The following privacy principles (as described in the privacy framework provided in ISO 29100) that should be applied are:

- Consent and choice;
- Purpose legitimacy and specification;
- Collection limitation;
- Data minimization;
- Use, retention and disclosure limitation;
- Accuracy and quality;
- Openness, transparency and notice;
- Individual participation and access;
- Accountability;
- Information security;
- Privacy compliance.

These principles need to be transposed by the assessment sponsor organization into privacy goals, functional requirements and key processes. They need to be implemented by the organization prior to assessing their privacy capability when using a context approach or a business function assessment approach as described in 5.1.

5.5 Prepare criteria for information collection

The criteria for information collection should be as follows:

a) Assessment of the level of privacy capability which is appropriate to the organization, given its purpose, function, risk assessment, etc.;

   The aim should be to create a short questionnaire (10-15 questions, aimed at senior stakeholders) which creates this “target” score for the organization;

b) Assessment of the actual, current levels of capability for each key process area in the organization;

   For each such key process area, the current capability level should be summarised in a paragraph explaining why one of the six defined levels has been assigned, and why the achievement level (see 4.4) has been assigned.

c) Advice on how to improve key process area capability levels to bring them from the "actual/observed" to the "target" level;

These recommendations and advice would be likely to depend on existing legislation and/or regulation and the potential impacts of non-compliance.

5.6 Collect and analyse information

ISO 33020 provides an approach for this using process attributes. Nine process attributes are defined and potential achievements identified.

Process Performance (PA 1.1):

- the process purpose is achieved.

Performance Management (PA 2.1):

- the performance of the process is managed.

Work Product Management (PA 2.2):

- the work products produced by the process are managed.

Process Definition (PA 3.1):

- a standard process is maintained to support the deployment of the defined process.

Process Deployment (PA 3.2):

- a standard process is deployed as a defined process to achieve its process outcomes;

Quantitative analysis (PA 4.1):

- information needs are defined, relationships between process elements are identified and data are collected.

Quantitative control (PA 4.2):

- objective data are used to manage process performance.

Process Innovation (PA 5.1):

- process improvement objectives not clearly defined;

- opportunities for improvement not clearly identified.

Process Innovation implementation (PA 5.2):

- inability to change process effectively to achieve relevant process improvement objectives;

- inability to evaluate effectiveness of process changes.

Each of the above process attributes consists of generic practices which are manifested as practice indicators. Appropriate attributes should be chosen for use when assessing process capability against target capability.

Table 1 shows which of the 9 process attributes apply to each of the capability scale levels (see 4.3).

Table 1 — Applicability of process attributes to assessment of capability levels

Capability Level	Process performance process	Performance management process	Work product management process	Process definition process	Process deployment process	Quantitative analysis process	Quantitative control process	Process innovation process	Process innovation implementation
Level 0: Incomplete									
Level 1: Performed	X								
Level 2: Managed	X	X	X						
Level 3: Established	X	X	X	X	X				
Level 4: Predictable	X	X	X	X	X	X	X		
Level 5: Innovating	X	X	X	X	X	X	X	X	X

5.7 Present results

Depending upon how the organization requires results to be presented to the appropriate audience, either a tabulated or descriptive report should be produced. The report should include details of:

- scope of the assessment;
- methodology used;
- who carried out the assessment and when;
- assessment results.

6 Example of a business function approach

Table 2 is an example of how the privacy-related capability levels against business functions can be recorded. The capability levels are based on those documented in 4.3 and the business functions are from the second example in 5.1.

Typically, this approach requires the assessment of each business process against each of the criteria outlined in Table 2.

Table 2 — Example of how to record capability levels against each business function

Date:							
Unit:							
Lead Assessor:							
Assessor							
Interviewee							
Ref.	Item Name	Item description	Further reference	Assessor Notes/evidence	Assessed capability level	Findings	References
1	Executive Oversight	How has unit implemented internal executive oversight and responsibility for data privacy and protection?	Unit Leadership acknowledges privacy accountability (e.g. appointment letter or other evidence). Issues are reported to respective Unit leaders and to Privacy Program Management. Issues are tracked. Privacy status of the unit is reported to Unit leadership periodically. Regular participation in the Privacy Program Management. Metrics exist and are reported. Escalation process has been defined to both unit and privacy program level. Annual Privacy implementation plan exists and it is monitored.			Major Findings: Minor Findings: Recommendations:	
2	Staffing & Delegation	How has unit allocated resources to ensure that the organisation's privacy programme is appropriately staffed by adequately trained personnel?	Privacy Owner and Officer(s) allocated and their role is recognized by Unit Leadership. Resources have adequate demonstrable competences. Role descriptions exist and are used in e.g. recruiting. Work is organized and staff understands their roles and responsibilities.			Major Findings: Minor Findings: Recommendations:	

Table 2 *(continued)*

3	Policies, Statements, Procedures, SOP, Requirements	How has unit demonstrated the existence of binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards?	Code of conduct refers to privacy and is published. XYZ Privacy Management Policy exists and is published. XYZ privacy vision and principles are known and used. XYZ wide privacy requirements exist and are used. Appropriate implementation guidelines and patterns exist, they cover relevant privacy topics, are up to date and used. Above documentation within the unit's responsibility is regularly reviewed and updated.			Major Findings: Minor Findings: Recommendations:	
4	Education & Awareness	How has unit provided for the up-to-date education and awareness of its employees and on-site contractors of data protection obligations?	Training and awareness approach and plans exists. Trainings are given to the target audiences as defined in XYZ Privacy Management Policy. Trainings are logged and reported. Relevant training materials exist and are available. Trainings are tailored for the audience. Industry and regulatory news are distributed to the privacy community.			Major Findings: Minor Findings: Recommendations:	
5	Risk Assessment & Mitigation	How has unit implemented a process to assist the organisation in understanding the risks to privacy raised by new products, services, technologies and business models, and to mitigate those risks?	Systematic and documented processes exist to identify and mitigate privacy concerns in products and services. Processes are comprehensive, i.e. the cover relevant business activities. Processes create documented evidence of compliance. Processes identify findings and make recommendations before go-live (where relevant). Non-compliant products with critical findings do not enter the market (without appropriate escalation). Completion of recommendations is monitored and critical un-closed deviations / major privacy risks are reported to respective unit leaders and to Privacy Program Management.			Major Findings: Minor Findings: Recommendations:	
6	Incident Request Handling	How has the unit integrated into the XYZ IRM process?	IRM process exists, and it is used to deal with issues. IRM unit contact, IRM training records, IRM unit SOP, Incident reports are maintained.			Major Findings: Minor Findings: Recommendations:	

Table 2 *(continued)*

7	Individual Participation & Redress	How has the unit created mechanisms for permitting consumers/employees to contact the unit's functional areas responsible for their products & services?	Users are given appropriate privacy notices. Information on how to contact XYZ for privacy matters is available to consumers / employees. CARE and HR personnel know how to handle typical requests and where to direct such requests internally. XYZ is capable to reply to and comply with such request within reasonable time, no longer than 30 days. Requests and replies are documented and documentation is available. Process is sufficiently documented.			Major Findings: Minor Findings: Recommendations:	
8	Other Procedures & Activities	How has the unit demonstrated the support and assurance of other privacy-related processes, procedures & activities?	Data inventory: Categories of data, data flows and processing practices thereto are documented. Such documentation is available to the privacy resources; Privacy statements are consistently published and updated when necessary in agreed languages through agreed channels; statements are documented and stored in quality repositories; process has an owner and it is documented. Industry and regulatory influence activities exists and they address identified hot topics in an effective manner; Governmental request for PII are managed according to relevant policies. Legal support: support is available. XYZ has the ability to track changes in legislation. Such information is made available and used. XYZ has necessary notifications to authorities in place.			Major Findings: Minor Findings: Recommendations:	

Bibliography

NOTE This section consists of an annotated list of relevant documents — including other standards documents applicable to the specific topic of privacy, and a pointer to appropriate Glossary/Terminology material. It is not the intention of this international standard to develop its own glossary. Where there is a need to use particular terms in a specific way (for instance "personal", "contextual integrity" etc.) which are not already reflected in a reference glossary, this international standard will include a definition of the term.

[1] ISO/IEC JTC 1/SC 27/WG5 SD2 *Official Privacy documents reference list*

[2] ISO/IEC 15288, *Systems and software engineering — System life cycle processes*

[3] ISO/IEC 21827, *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)*

[4] ISO/IEC 24745, *Information technology — Security techniques — Biometric information protection*

[5] ISO/IEC 24760, *Information technology — Security techniques — A framework for identity management*

[6] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

[7] ISO/IEC 29191, *Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication*

[8] ISO/IEC 33002:2015, *Information technology — Process assessment — Requirements for performing an assessment*

[9] ISO/IEC 33003:2015, *Information technology — Process assessment — Requirements for process management frameworks*

[10] ISO/IEC 33004:2015, *Information technology — Process assessment — Requirements for process reference, process assessment and maturity models*

[11] Privacy Maturity Model published by AICPA/CICA, see http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/generallyacceptedprivacyprinciples/downloadabledocuments/aicpa-cica-privacy-maturity-model-ebook.pdf

[12] Implementing Accountability in the Marketplace - A Discussion Document, published by CIPL, Appendix B (Common Fundamentals of an Accountability Implementation Programme) see http://www.hunton.com/files/Uploads/Documents/Centre/Centre_Accountability_Phase_III_White_Paper.pdf

ICS 35.040

Price based on 15 pages