

BS 10012:2017+A1:2018



BSI Standards Publication

Data protection — Specification for a personal information management system



Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2018

Published by BSI Standards Limited 2018

ISBN 978 0 539 01173 9

ICS 01.140.30; 03.100.99; 23.040.20; 23.040.45; 35.020

The following BSI references relate to the work on this document:

Committee reference IDT/1

Draft for comment 18/30378573 DC

Amendments/corrigenda issued since publication

Date	Text affected
July 2018	See Foreword

Contents

	Page
Foreword	ii
0 Introduction	1
1 Scope	3
2 Normative references	3
3 Terms, definitions and abbreviations	3
4 Context of the organization	8
5 Leadership	9
6 Planning	11
7 Support	16
8 Operation	18
9 Performance evaluation	35
10 Improvement	36
Annex A (informative) ISO standardized management system	38
Annex B (informative) Comparison between the GDPR 2016 [1] and UK practice under the DPA 1998 [3]	39
<i>Table B.1 — Comparison between the GDPR 2016 [1] and UK practice under the DPA 1998 [3]</i>	39
Annex C (informative) Codes, seals, certifications and trust marks	41
Bibliography	42

Summary of pages

This document comprises a front cover, and inside front cover, pages i to ii, pages 1 to 43, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 31 March 2017. It was prepared by Technical Committee IDT/1, *Data protection*. A list of organizations represented on this committee can be obtained on request to its secretary.

Supersession

BS 10012:2017+A1:2018 supersedes BS 10012:2017, which is withdrawn.

Information about this document

This is a full revision of the standard, and introduces the following principal changes:

- requirements have been revised in line with the European Union General Data Protection Regulation 679/2016 (GDPR [1])¹;
- the structure has been updated to follow the ISO management system structure (see [Annex A](#)).

The start and finish of text introduced or altered by Amendment No.1 is indicated in the text by tags **A1** and **A1**. Minor editorial changes are not tagged.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is “shall”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Requirements in this standard are drafted in accordance with *Rules for the structure and drafting of UK standards*, subclause **J.1.1**, which states, “Requirements should be expressed using wording such as: ‘When tested as described in [Annex A](#), the product shall ...’”. This means that only those products that are capable of passing the specified test will be deemed to conform to this standard.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

¹ See http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf [last accessed on 10 March 2017].

0 Introduction

0.1 General

The objective of this British Standard is to enable organizations to put in place, as part of the overall information governance infrastructure, a personal information management system (PIMS) which provides a framework for maintaining and improving compliance with data protection requirements and good practice.

In many cases, a PIMS will address the management of personal information that is held across a wide range of operational units and information technology based application systems. Much of this personal information might also be within the scope of other management systems within the organization [e.g. quality management (BS EN ISO 9001), environmental management (BS EN ISO 14001), asset management ([ISO 55001](#)), information security management ([BS EN ISO/IEC 27001](#))]. Where the organization has such multiple overlapping management systems, consideration needs to be given to utilizing a common approach such as that described in [PAS 99](#), *Specification of common management system requirements as a framework for integration*.

This new edition of BS 10012 has been written in recognition of the publication of the European Union General Data Protection Regulation (GDPR) [[1](#)], which was approved by the European Parliament on 14 April 2016. This replaces the European Directive (95/46/EC) on 25 May 1996 [[2](#)], which was implemented in the UK by the Data Protection Act 1998 [[3](#)]. The GDPR will be directly applicable to the UK and member states retain the ability to introduce national level derogations where these are required for specific purposes. However the results of the referendum on the UK's membership of the European Union make it unclear how the GDPR will be implemented – such issues will be monitored and updates to this British Standard will be issued where necessary.

NOTE 1 [Annex B](#) compares UK practice under the DPA 1998 [[3](#)] and the GDPR 2016 [[1](#)].

Compliance with EU and UK data protection legislation is monitored, regulated and enforced by the Information Commissioner (the UK's "supervisory authority"), who is responsible for promoting the protection of personal information. The Information Commissioner promotes good practice by the issue of guidance, rules on eligible complaints, provides information to individuals and organizations (acting as controllers and/or processors) and takes appropriate action when the law is broken. The Information Commissioner has powers to investigate complaints, make assessments as to whether processing is compliant with the national legislation, and issue information and enforcement notices.

NOTE 2 Articles 57 and 58 of the GDPR [[1](#)] detail the requirements and powers for supervisory authorities.

This British Standard is drafted using the rules specified for management system standards in the ISO Directives, Annex SL, and follows the common structure and core text (see [Annex A](#)). This enables compatibility with ISO management system standards.

0.2 Data protection principles

The GDPR requires personal information to be processed according to six data protection principles², which require personal information to be:

- a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are, in accordance with Article 89(1), not considered to be incompatible with the initial purposes ("purpose limitation");

² The text given here is a summary of Article 5 of the GDPR [[1](#)]. For the full text, see the GDPR.

- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization");
- d) accurate and, where necessary, kept up to date; every reasonable step is taken to ensure that personal information that is inaccurate, with regard to the purposes for which it is processed, is erased or rectified without delay ("accuracy");
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information is processed; personal information can be stored for longer periods so far as the personal information is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject ("storage limitation"); and
- f) processed in a manner that ensures appropriate security of the personal information, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality").

There is a seventh principle which requires data controllers to be accountable for, and be able to demonstrate compliance with, the six principles above.

In summary:

- Principle (a) Lawfully, fairly and transparently processed (see [8.2.6](#));
- Principle (b) Obtained only for specific legitimate purposes (see [8.2.7](#));
- Principle (c) Adequate, relevant, limited in line with data limitation principles (see [8.2.8](#));
- Principle (d) Accurate and up to date, with every effort to erase or rectify without delay (see [8.2.9](#));
- Principle (e) Stored in a form that permits identification no longer than necessary (see [8.2.10](#));
- Principle (f) Ensure appropriate security, integrity and confidentiality of personal information using technological and organizational measures (see [8.2.11](#)).
- General Accountability for the above

A number of exemptions or derogations from these data protection principles are permitted by the GDPR and can be introduced in national legislation. Examples of such exemptions are the processing for journalistic, academic, artistic and/or literary expression purposes.

NOTE See Recital 153 of the GDPR [1].

Reference can be made to the GDPR, national legislation, guidance from the supervisory authority and to other guidance and sector-specific advice for further details.

0.3 Notification

[A1] General notification obligations are not required under the GDPR. However, the UK government has announced a new charging structure for data controllers, see the Digital Economy Act 2017 [4]. The UK Data Protection Act 2018 (Section 137) [5] gives information regarding charges that will be payable to the Information Commissioner. For further details of these charges, see <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/10/blog-ico-fee-and-registration-changes-next-year/>³. **[A1]**

³ Last accessed on 31 July 2018.

1 Scope

This British Standard specifies requirements for a personal information management system (PIMS), which provides a framework for maintaining and improving compliance with data protection requirements and good practice.

This British Standard is for use by organizations of any size and sector. It is intended to be used by those responsible for planning, establishing, implementing and maintaining a PIMS within an organization. It is intended to provide a common ground for the responsible management of personal information, for providing confidence in its management, and for enabling an effective assessment of compliance with data protection requirements and good practice by both internal and external assessors.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1 audit

systematic, independent and documented *process* (3.1.28) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

NOTE 1 An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

NOTE 2 An internal audit is conducted by the organization itself, or by an external party on its behalf.

NOTE 3 "Audit evidence" and "audit criteria" are defined in BS EN ISO 19011.

3.1.2 biometric information

personal information resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a *natural person* (3.1.17)

NOTE Biometric information typically allows or confirms the unique identification of the natural person, using information such as facial images or dactyloscopic data (such as finger prints).

3.1.3 competence

ability to apply knowledge and skills to achieve intended results

3.1.4 conformity

fulfilment of a *requirement* (3.1.31)

3.1.5 continual improvement

recurring activity to enhance *performance* (3.1.22)

3.1.6 corrective action

action to eliminate the cause of a *nonconformity* (3.1.18) and to prevent recurrence

A1 3.1.7 data breach

breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed **A1**

A1 3.1.8 data controller

organization ([3.1.20](#)) that decides means and purpose of how personal information are processed **A1**

A1 3.1.9 data processor

organization ([3.1.20](#)) that only follows instructions from a data controller ([3.1.8](#)) but who has obligations towards security (e.g. breach reporting) **A1**

3.1.10 documented information

information required to be controlled and maintained by an *organization* ([3.1.20](#)) and the medium on which it is contained

NOTE 1 Documented information can be in any format and media, and from any source.

NOTE 2 Documented information can refer to:

- the management system ([3.1.14](#)), including related processes ([3.1.28](#));
- information created in order for the organization to operate (documentation);
- evidence of results achieved (records).

3.1.11 effectiveness

extent to which planned activities are realized and planned results achieved

3.1.12 genetic information

personal information relating to the inherited or acquired genetic characteristics of a *natural person* ([3.1.17](#))

NOTE Genetic information typically includes unique information about the physiology which can indicate the health of the natural person and which results, in particular, from an analysis of a biological sample from the natural person in question.

3.1.13 interested party (preferred term) stakeholder (admitted term)

person or *organization* ([3.1.20](#)) that can affect, be affected by, or perceive itself to be affected by a decision or activity

NOTE Examples of relevant persons include workers, citizens, patients, consumers and users.

3.1.14 management system

set of interrelated or interacting elements of an *organization* ([3.1.20](#)) to establish *policies* ([3.1.26](#)) and *objectives* ([3.1.19](#)) and *processes* ([3.1.28](#)) to achieve those objectives

NOTE 1 A management system can address a single discipline or several disciplines.

NOTE 2 The system elements include the organization's structure, roles and responsibilities, planning and operation.

NOTE 3 The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

3.1.15 measurement

process (3.1.28) to determine a value

3.1.16 monitoring

determining the status of a system, a process (3.1.28) or an activity

NOTE To determine the status, there might be a need to check, supervise or critically observe.

3.1.17 natural person (data subject)

living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity ^{A1} from information in the possession of, or likely to come into possession of the organization ^{A1}

NOTE Extracted from the definition of "personal data" in Article 4(1) of the GDPR [1].

3.1.18 nonconformity

non-fulfilment of a requirement (3.1.31)

3.1.19 objective

result to be achieved

NOTE 1 An objective can be strategic, tactical, or operational.

NOTE 2 Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process (3.1.28)).

NOTE 3 An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a PIMS objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

NOTE 4 In the context of PIMS, PIMS objectives are set by the organization, consistent with the PIMS policy, to achieve specific results.

3.1.20 organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives (3.1.19)

NOTE 1 The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

EXAMPLE Natural persons, sole traders, companies, partnerships, bodies corporate, public sector bodies, voluntary associations and charities.

^{A1} *NOTE 2 An organization can be either a data controller (3.1.8), a data processor (3.1.9) or both depending on the processing undertaken (3.1.29). ^{A1}*

3.1.21 outsource (verb)

make an arrangement where an external organization (3.1.20) performs part of an organization's function or process (3.1.28)

NOTE An external organization is outside the scope of the management system (3.1.14), although the outsourced function or process is within the scope.

3.1.22 performance

measurable result

NOTE 1 Performance can relate either to quantitative or qualitative findings.

NOTE 2 Performance can relate to the management of activities, processes (3.1.28), products (including services), systems or organizations (3.1.20).

3.1.23 personal information

information relating to an identified or identifiable *natural person* (3.1.17)

NOTE 1 An identifiable person is one who can be identified directly or indirectly, in particular with reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

NOTE 2 This includes pseudonymized but not fully anonymized data.

NOTE 3 Article 4(1) of the GDPR [1] defines "personal data" in this manner.

3.1.24 personal information management policy

statement of overall intentions and direction of the organization as formally approved by top management for managing compliance with data protection requirements and good practice

NOTE Hereafter referred to as "PIMS policy".

3.1.25 personal information management system (PIMS)

part of the overall management framework that plans, establishes, implements and maintains the management of personal information

NOTE It is recognized that an organizational PIMS addresses the management of personal information that might be held across a wide range of operational units and information technology based applications systems.

3.1.26 policy

intentions and direction of an *organization* (3.1.20), as formally expressed by its *top management* (3.1.36)

3.1.27 procedure

documented set of actions which is the prescribed or accepted way of doing something

3.1.28 process

set of interrelated or interacting activities which transforms inputs into outputs

3.1.29 processing

operation or set of operations which is performed upon personal information or sets of personal information

NOTE This is irrespective of whether or not by automated means.

EXAMPLES Processing can include collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (from the GDPR [1], Article 4(2)).

3.1.30 profiling

form of automated processing of personal information consisting of the use of personal information to evaluate certain personal aspects relating to a *natural person* (3.1.17)

NOTE Profiling is often used to analyse or predict aspects concerning that *natural person's* performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

3.1.31 requirement

need or expectation that is stated, generally implied or obligatory

NOTE 1 “Generally implied” means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

NOTE 2 A specified requirement is one that is stated, for example in documented information.

3.1.32 risk

effect of uncertainty

NOTE 1 An effect is a deviation from the expected — positive or negative.

NOTE 2 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

NOTE 3 Risk is often characterized by reference to potential “events” (as defined in PD ISO Guide 73:2009, 3.5.1.3) and “consequences” (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated “likelihood” (as defined in PD ISO Guide 73:2009, 3.6.1.1) of occurrence.

3.1.33 special categories of personal information

personal information (3.1.23) relating to the natural person’s (3.1.17):

- a) racial or ethnic origin;
- b) political opinions;
- c) religious or philosophical beliefs;
- d) trade-union membership;
- e) the processing of genetic information;
- f) biometric information for the purpose of uniquely identifying a natural person;
- g) information concerning health or information concerning a natural person's sex life or sexual orientation.

NOTE 1 See Article 9 of the GDPR [1] for special conditions under which special category information can be processed.

A1 *NOTE 2* Criminal offences, alleged offences and related proceedings are not special categories of personal information, but should be treated in the same way. **A1**

3.1.34 system

set of interrelated or interacting elements

[SOURCE: BS EN ISO 9000:2015, 3.5.1]

3.1.35 third party

natural or legal person, public authority, agency or body other than the data subject, data controller, data processor and workers who, under the direct authority of the data controller or data processor, are authorized to process personal information

[SOURCE: Adapted from Article 4(10) of the GDPR[1]]

3.1.36 top management

person or group of people who directs and controls an organization (3.1.20) at the highest level

NOTE 1 Top management has the power to delegate authority and provide resources within the organization.

NOTE 2 If the scope of the management system (3.1.14) covers only part of an organization, then top management refer to those who direct and control that part of the organization.

3.1.37 workers

people working under the control of the organization

NOTE 1 This includes employees, temporary staff, contractors, volunteers and consultants.

NOTE 2 This also includes top management.

3.2 Abbreviations

BCR	Binding Corporate Rules
DPA	Data Protection Act 1998 [3]
DPO	Data Protection Officer
EEA	European Economic Area
EU	European Union
FCA	Financial Conduct Authority
GDPR	General Data Protection Regulation [1]
ICO	Information Commissioner's Office
PIA	Privacy Impact Assessment
PIMS	Personal Information Management System

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its personal information management system.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

- the interested parties that are relevant to the PIMS;
- the relevant requirements of these interested parties.

4.3 Determining the scope of the personal information management system

The organization shall determine the boundaries and applicability of the PIMS to establish its scope.

When determining this scope, the organization shall consider:

- the external and internal issues referred to in 4.1;
- the requirements referred to in 4.2;
- organizational objectives and obligations;
- the organization's acceptable level of risk; and
- applicable statutory, regulatory, contractual and/or professional duties.

The scope shall be available as documented information.

4.4 Personal information management system

Objective: To plan for the implementation of a PIMS that can provide direction and support for compliance with data protection requirements and good practice.

The organization shall establish, implement, maintain and continually improve a PIMS, including the processes needed and their interactions, in accordance with the requirements of this British Standard.

NOTE It is recognized that an organizational PIMS addresses the management of personal information that might be held across a wide range of operational units and information technology based applications systems. Much of this personal information might also be within the scope of other management systems within the organization (e.g. quality management (BS EN ISO 9001), environmental management (BS EN ISO 14001), asset management (BS EN ISO 55001), information security management (BS EN ISO/IEC 27001)). Where the organization has such multiple, overlapping management systems consideration should be given to utilizing an approach such as described in PAS 99, Specification of common management system requirements as a framework for integration.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the PIMS by:

- ensuring that the PIMS policy and PIMS objectives are established and are compatible with the strategic direction of the organization;
- ensuring the integration of the PIMS requirements into the organization's business processes;
- ensuring that the resources needed for the PIMS are available;
- communicating the importance of effective personal information management and of conforming to the PIMS requirements;
- ensuring that the PIMS achieves its intended outcome(s);
- directing and supporting persons to contribute to the effectiveness of the PIMS;
- promoting continual improvement;
- supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this British Standard can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Policy

Top management shall establish a PIMS policy that:

- a) is appropriate to the purpose of the organization;
- b) provides a framework for setting PIMS objectives;
- c) includes a commitment to satisfy applicable requirements;
- d) includes a commitment to continual improvement of the PIMS management system.

The PIMS policy shall:

- be available as documented information;
- be communicated within the organization;
- be available to interested parties, as appropriate.

The PIMS policy shall state the organization's commitment to compliance with data protection requirements and good practice, including:

- 1) processing personal information only where this is strictly necessary for legal and regulatory purposes, or for legitimate organizational purposes (see [6.1.3.1](#));
- 2) processing only the minimum personal information required for these purposes (see [6.1.7](#));
- 3) providing clear information to natural persons (including children) about how their personal information can be used and by whom (see [8.2.12.2](#));
- 4) ensuring special safeguards when collecting information directly from children (see [6.1.4](#), [8.2.2.2](#), [8.2.7.3](#) and [8.2.7.6](#));
- 5) only processing relevant and adequate personal information (see [8.2.8](#));
- 6) processing personal information fairly and lawfully (see [8.2.6](#));
- 7) maintaining a documented inventory of the categories of personal information processed by the organization (see [8.2.2.1](#));
- 8) keeping personal information accurate and, where necessary, up-to-date (see [8.2.9.1](#));
- 9) retaining personal information only for as long as is necessary for legal or regulatory reasons or for legitimate organizational purposes and ensuring timely and appropriate disposal (see [8.2.10](#));
- 10) respecting natural persons' rights in relation to their personal information (see [8.2.12](#));
- 11) keeping all personal information secure (see [8.2.11](#));
- 12) only transferring personal information outside the UK in circumstances where it can be adequately protected (see [8.2.11.8](#));
- 13) where appropriate, the strategy for dealing with regulators across the EU, where goods and/or services are offered to natural persons who are resident in other EU countries  (see [8.2.11.11](#)) ;
- 14) the application of the various exemptions allowable by data protection legislation;
- 15) developing and implementing a PIMS to enable the PIMS policy to be implemented (see [6.1](#), [6.2](#) and [7](#));
- 16) where appropriate, identifying internal and external interested parties and the degree to which they are involved in the governance of the organization's PIMS (see [7.4](#));
- 17) the identification of workers with specific responsibility and accountability (see [3.1.34](#) and [8.2.1](#)) for the PIMS; and
- 18) maintain records of processing of personal information (see [8.2.6.1](#), [8.2.6.2](#), [8.2.7.2](#), [8.2.11.7](#) and [8.2.11.9](#)).

The PIMS policy shall state that it covers either:

- the whole organization; or
- an identified part of the organization.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

- a) ensuring that the PIMS conforms to the requirements of this British Standard;
- b) reporting on the performance of the PIMS to top management.

A member of the top management team shall be accountable for the management of personal information within the organization so that compliance with data protection requirements and good practice can be demonstrated (see also [8.2.1.1](#), [A1](#) [8.2.1.2](#) [A1](#)). This accountability shall include:

- 1) approval of the PIMS policy by the top management team;
- 2) development and implementation of the PIMS as required by the PIMS policy; and
- 3) security and risk management in relation to compliance with the PIMS policy (see also [8.2.11.1](#)).

One or more suitably qualified or experienced workers shall be appointed to take responsibility for the organization's compliance with the PIMS policy on a day-to-day basis (see also [8.2.1.3](#)).

NOTE The senior manager accountable and the worker(s) responsible for day-to-day compliance could be the same person.

Workers shall comply with the PIMS policy by the implementation of the organization's processes and procedures, with sanctions, appropriate worker development, or procedures put in place to respond to any nonconformities.

5.4 Embedding the PIMS in the organization's culture

To ensure that the management of personal information becomes a part of the organization's core values and effective management, the organization shall:

- a) raise, enhance, test and maintain awareness of the PIMS through an ongoing education and awareness programme for workers;
- b) establish a process for evaluating the effectiveness of the PIMS awareness delivery;
- c) communicate to workers the importance of:
 - 1) meeting PIMS objectives;
 - 2) complying with the PIMS policy;
 - 3) continual improvement of the PIMS policy;
- d) ensure that workers are aware of how they contribute to the achievement of the organization's PIMS objectives and the consequences of nonconformity; and
- e) retain documented information of training and awareness activities and its effectiveness.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the PIMS, the organization shall consider the issues referred to in [4.1](#) and the requirements referred to in [4.2](#) and determine the risks and opportunities that need to be addressed to:

- give assurance that the PIMS can achieve its intended outcome(s);
- prevent, or reduce, undesired effects;
- achieve continual improvement.