PAS 99:2006

PUBLICLY AVAILABLE SPECIFICATION

Specification of common management system requirements as a framework for integration

ICS 03.100.99

Publishing and copyright information

ISBN 0 580 49059 9

Publication history

First edition, 31 August 2006

Amendments issued since publication

Amd. no.	Date	Text affected

Contents

Summary of pages

This document comprises a front cover, an inside front cover, pages i to vi, pages 1 to 20, an inside back cover and a back cover.

Foreword

This Publicly Available Specification (PAS) has been prepared by the British Standards Institution (BSI) in partnership with BSI Management Systems. It is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

Acknowledgement is given to the following members of a specially constituted Steering Group, who were involved in the drafting of this specification.

John Hele, BSI Management Systems
David Smith, IMS Risk Solutions
Tara West, BSI Professional Standards
Martin Baxter, Institute of Environmental Management and Assessment (IEMA)
Brian Burroughs, Independent International Organization for Certification (IIOC)
Steve Dewhirst, Association of British Certification Bodies
Dick Hortensius, Netherlands Standards Institute (NEN)
Marijke Korteweg, Institute of Quality Assurance
John Parkinson, British Chemical Distribution Association
Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this specification.

Organizations should use this PAS in conjunction with the specific requirements of management system standards or specifications to which the organization subscribes e.g. ISO 9001, ISO 14001, ISO/IEC 27001, ISO 22000, ISO/IEC 20000 and OHSAS 18001.

Adherence to this PAS does not ensure conformity with any management system standard or specification.

Compliance with a Publicly Available Specification does not of itself confer immunity from legal obligations.

Introduction

Many organizations have adopted or are adopting formal management system standards and/or specifications such as ISO 9001, ISO 14001, ISO/IEC 27001, ISO 22000, ISO/IEC 20000 and OHSAS 18001.

Frequently these are operated as independent systems. In all management systems, however, there are certain common elements which can be managed in an integrated way; the essential unity of all these systems within the overall management system of the organization can then be recognized and used to best advantage. Therefore organizations are questioning the approach of having separate systems.

To accommodate the growing interest in an integrated approach to management systems and the governance of organizational risk, this specification defines common management system requirements. It is intended to be used as a framework for implementing common requirements of management system standards or specifications in an integrated way.

PAS 99 is primarily meant to be used by those organizations who are implementing the requirements of two or more management system standards. The adoption of this PAS is intended to simplify the implementation of multiple system standards and any associated conformity assessment.

Organizations using this PAS should include as input, the specific requirements of management system standards or specifications to which they subscribe e.g. ISO 9001, ISO 14001, ISO/IEC 27001, ISO 22000, ISO/IEC 20000 and OHSAS 18001.

Compliance with this PAS does not in itself ensure conformity with any other management system standards or specifications. The particular requirements of each management system standard will still need to be addressed and satisfied if certification, where sought, is to be achieved. Certification to this PAS in its own right is not appropriate.

This PAS has been produced to help organizations to achieve benefits from consolidating the common requirements in all management system standards/specifications and managing these requirements effectively. The benefits may include:

a) improved business focus;

b) a more holistic approach to managing business risks;

c) less conflict between systems;

d) reduced duplication and bureaucracy;

e) more effective and efficient audits both internally and externally.

ISO Guide 72 [1] for standards writers includes a framework for the common requirements that are found in management system standards. The main requirements are categorized into the following subjects:

a) Policy;

b) Planning;

c) Implementation and operation;

d) Performance assessment;

e) Improvement;

f) Management review.

Each management system standard has its own specific requirements, but these six subjects will be present in all of them and can be adopted as the basis for integration. This PAS therefore uses the same categorization as a framework for the common management system requirements and each subject will be considered in more detail in the course of this specification.

Many of the requirements in standards/specifications are common and these can be practically accommodated under one generic management system as shown in Figure 1. It follows that the reduction in duplication by combining two or more systems in this way has the potential to significantly reduce the overall size of the management system and improve system efficiency and effectiveness.

Figure 1 **Illustration of how the common requirements of multiple management system standards/specifications can be integrated into one common system**

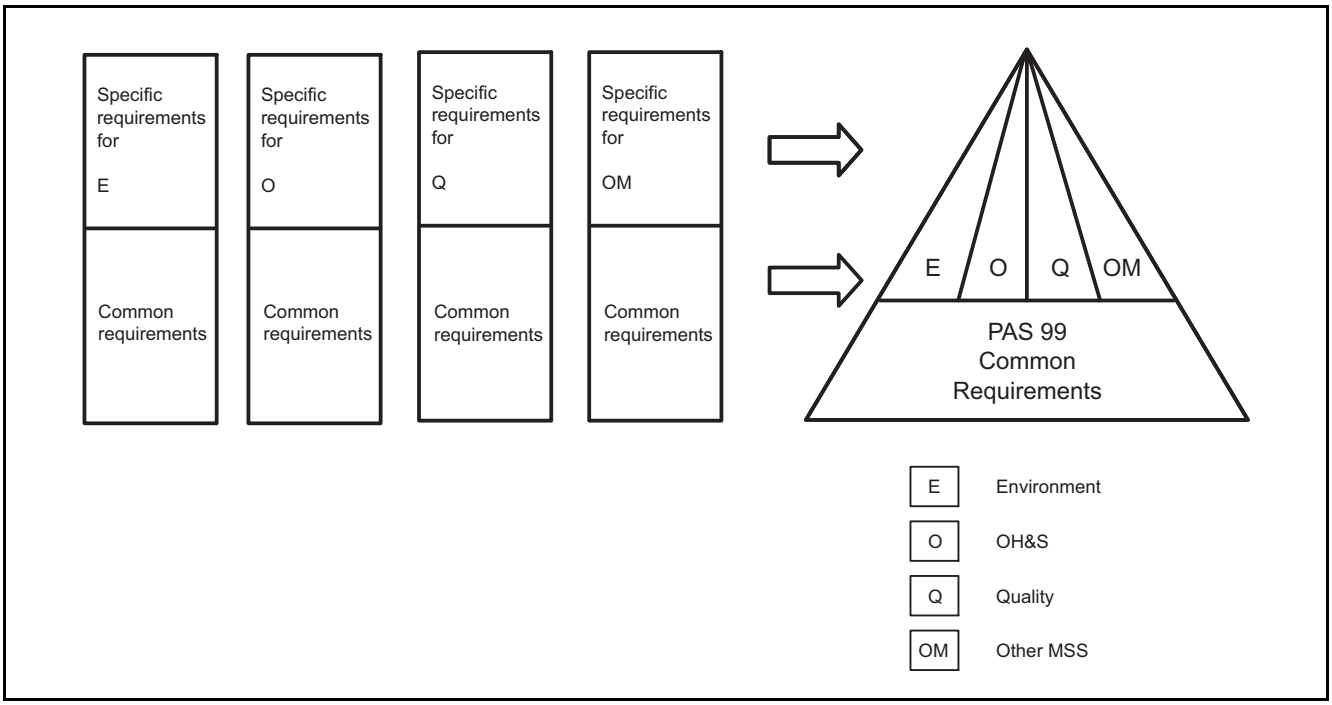
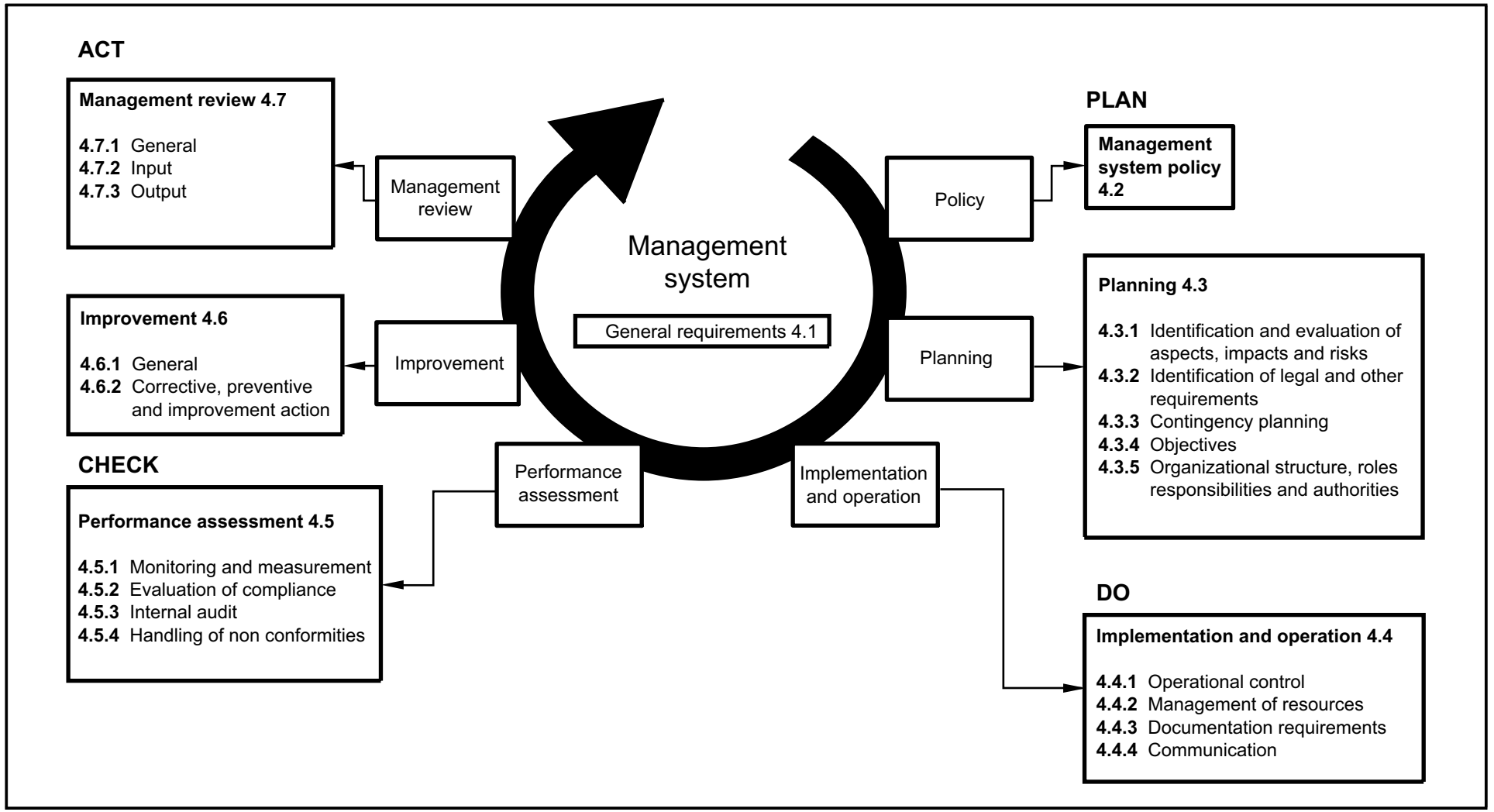


Figure 1 shows that if the various management system requirements can be so arranged that the core requirements are addressed in a common way, it is possible to integrate the systems to the degree that is most appropriate to the organization whilst minimizing duplication.

The framework used in the PAS is based on ISO Guide 72 [1] with some modifications, and has been tested in practice. It applies to all management systems whether they are the subject of a formal management system standard or whether they are less formal systems which form part of the overall management system of the organization. The six common requirements mentioned above should be looked at in conjunction with Plan, Do, Check, Act, which all management systems follow. Figure 2 illustrates how PDCA and the common requirements combine to give the outline structure of the management system.

The model used is as follows:

Figure 2 **Illustration of how PDCA and the common requirements combine to give the outline structure of the management system**



Integration should be planned and implemented in a structured way. Many businesses have adopted management system standards as a result of outside pressures such as customers demanding the implementation of a quality standard or external requirements to install an occupational health and safety system. This does not apply to integration, which will be done purely for the benefit of the business. The first step should therefore be to identify the business needs. If a business does not see benefits from integration, then it should not do it – although it is difficult to imagine an organization that would not see benefits arising.

To meet the requirements of a specific management system standard it will be necessary to carry out an analysis of the requirements in detail and compare them with those that have already been incorporated in the integrated system. Even elements which are considered common may have subtle differences within the content of the individual standard/specification.

1 Scope

This PAS specifies common management system requirements and is intended to be used as a framework for implementing two or more management system standards/specifications in an integrated way. It draws together the common requirements in management system standards/specifications.

Although it is primarily intended to be used in combination with management system standards/specifications such as ISO 9001, ISO 14001, ISO/IEC 27001, ISO 22000, ISO/IEC 20000 and/or OHSAS 18001 it can also be used with other national and international management system standards/specifications.

It applies to all sizes and types of organization.

It is not intended for organizations that have based their management system upon a single standard/specification except as preparation for the adoption of additional systems or standards.

Compliance with this PAS does not ensure compliance with any other management system standards/specifications.

2 Normative references

Only the standards/specifications that the organization subscribes to and that it wants to use in combination with this PAS apply as normative references. Those listed below are examples of standards/specifications that may be combined with the use of this PAS but other national and international managment system standards/specifications may be considered as appropriate to the organization's needs.

Users of this PAS are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements.*

ISO/IEC 20000:2005, *Information technology – Service management.*

ISO 9001:2000, *Quality management systems – Requirements.*

ISO 14001:2004, *Environmental management systems – Requirements with guidance for use.*

ISO 22000:2005, *Food safety management systems – Requirements for any organization in the food chain.*

OHSAS 18001:1999, *Occupational health and safety management systems – Specifications.*

3 Terms and definitions

For the purposes of this PAS, the following terms and definitions apply. The definitions of the management systems standards and/or specifications used in combination with this PAS shall take precedence.

3.1 aspect
characteristic of an activity, product or service that has or can have an **impact** (see **3.4**)

NOTE 1 See **A.4.3.2** *for additional explanation of this concept.*

NOTE 2 A significant aspect has or can have a significant impact.

3.2 contingency planning
consideration of the potentially serious incidents that could affect the operations of the organization and the formulation of a plan(s) to prevent or mitigate the effects and to enable the organization to operate as normally as possible

3.3 document
information and its supporting medium

NOTE 1 The medium can be paper, magnetic, electronic or optical computer disc, photograph or master sample, or a combination thereof.

NOTE 2 A set of documents, for example specifications or records, is frequently called "documentation".

3.4 impact
effect on the organization's policy commitments and objectives, its interested parties, the organization itself and/or on the environment

NOTE An effect can be positive or negative.

3.5 interested party
person or group concerned with or affected by the activities, products and/or services of an organization

NOTE 1 This could include customers, owners, regulators, non governmental organizations (NGO), people in an organization, suppliers, bankers, unions, partners or society.

NOTE 2 A group can comprise an organization, a part thereof or more than one organization.

3.6 management system
system(s) to establish policy and objectives and to achieve those objectives

NOTE A management system comprises the elements of policy, planning, implementation and operation, performance assessment, improvement and management review (see Figure 2).

3.7 procedure
specified way to carry out an activity or a process

NOTE Procedures can be documented or not.

3.8 process
set of interrelated or interacting activities which transforms inputs into outputs

NOTE Processes may be classified in a number of different ways. A distinction is sometimes made between operational processes which are directly concerned with the planned outputs of the organization, and management processes which provide the framework that enables the operational processes to take place.

3.9 risk
likelihood of an event occurring that will have an impact on objectives

NOTE 1 Risk is normally determined in terms of combination of the likelihood of an event and its consequences.

*NOTE 2 An event may be the occurrence of an **aspect** (see* **3.1***) with the associated **impact** (see* **3.4***) as its consequence.*

NOTE 3 See **A.3** *for additional explanation of risk.*

4 Common management system requirements

4.1 General requirements

4.1.1 The organization shall document the scope of the management system and the management system standards/specifications to which it subscribes.

4.1.2 The organization shall establish, document, implement, maintain and continually improve the management system in accordance with the requirements of this PAS and the management system standards/specifications to which it subscribes.

4.1.3 In order to meet its declared policies and objectives, the organization shall:

a) identify the processes needed for the implementation, operation and maintenance of the management system, and their application throughout the organization;

b) determine the sequence and interaction of these processes and the applicability for integration of these processes;

c) determine criteria and methods needed to ensure that both the operation and control of these processes are effective;

d) ensure the availability of resources and information necessary to support the operation and monitoring of these processes;

e) monitor, measure and analyse these processes, and implement actions necessary to achieve planned results and continual improvement of the organization's overall performance.

4.2 Management system policy

Top management shall define the policy of the organization in respect of its management system and ensure that it:

a) is appropriate to the organization's activities, products and services;

b) includes a commitment to comply with all relevant legal and other requirements to which the organization subscribes and to continually improve the effectiveness of the management system;

c) provides a framework for establishing and reviewing objectives;

d) is communicated to all persons working for or on behalf of the organization;

e) is regularly reviewed for continuing suitability.

NOTE Organizations may have a specific policy covering each management system standard that it subscribes to or may combine all of the policy requirements into one policy.

4.3 Planning

4.3.1 Identification and evaluation of aspects, impacts and risks

The organization shall establish, implement and maintain (a) procedure(s):

a) to identify the aspects of its activities, products and services relevant to the scope of the management system;

b) to evaluate the risks to the organization by determining and recording those aspects that have or can have a significant impact (i.e significant aspects).

The organization shall ensure that the significant aspects are considered when establishing, implementing and maintaining its management system.

4.3.2 Identification of legal and other requirements

The organization shall establish, implement and maintain (a) procedure(s) to determine the legal and other requirements relating to its activities, products and services that are relevant to the scope of the management system and take them into account when establishing, implementing and maintaining its management system.

4.3.3 Contingency planning

The organization shall establish, document and maintain (a) procedure(s) for identifying and responding to any unplanned event, potential emergency or disaster. This procedure(s) shall seek to prevent or mitigate the consequences of any such occurrence and consider the continuity of the business operations.

4.3.4 Objectives

4.3.4.1 The organization shall establish objectives, taking into account its significant aspects, legal obligations, other applicable requirements and its commitment to continual improvement when implementing its policy. These objectives shall be measurable.

4.3.4.2 The organization shall establish, implement and maintain (a) programme(s) for achieving its objectives.

4.3.5 Organizational structure, roles, responsibilities and authorities

4.3.5.1 The organization's top management shall appoint (a) specific management representative(s) who, irrespective of other responsibilities, shall have defined roles, responsibilities and authority for:

a) ensuring that the management system is established, implemented and maintained in accordance with the requirements of this PAS and the management system standards/specifications to which the organization subscribes;

b) reporting to top management on the performance of the management system for review, including recommendations for improvement.

4.3.5.2 The organization shall identify, document and communicate the roles, responsibilities and authorities of those involved in the management system and their interrelationships within the organization.

4.4 Implementation and operation

4.4.1 Operational control

The organization shall ensure that the operations that are associated with significant aspects are carried out under specified conditions in order to meet the organization's policies and objectives as well as legal and other applicable requirements.

4.4.2 Management of resources

4.4.2.1 The organization shall ensure that all people working for or on behalf of the organization are competent on the basis of appropriate education, training, skills and experience for the tasks assigned to them.

4.4.2.2 The organization shall:

a) evaluate the effectiveness of the actions taken to ensure competence;

b) ensure that its personnel are aware of the relevance and importance of their activities and how they contribute to the achievement of the objectives.

4.4.2.3 The organization shall determine, provide and maintain the resources and infrastructure needed to achieve its objectives.

4.4.3 Documentation requirements

4.4.3.1 The management system documentation shall include:

a) a description of the scope of the management system, including the management systems standards/specifications subscribed to;

b) statements of the organization's policies and objectives;

c) a system manual describing the main elements of the management system and their interaction, including common policies, processes and procedures and references to related documents;

d) the documented procedures and records that are required by this PAS and the management system standards/specifications to which the organization subscribes;

e) documents determined as necessary by the organization to ensure the effective planning, operation and control of its processes.

4.4.3.2 Documents required by the management system shall be controlled.

4.4.3.3 The organization shall establish, implement and maintain (a) documented procedure(s) to define the controls needed to:

a) approve documents for adequacy prior to issue;

b) review and update and re-approve documents as necessary;

c) ensure that changes and current revision status of documents are identified;

d) ensure that relevant versions of applicable documents are available at points of use;

e) ensure that documents remain legible and readily identifiable;

f) ensure that documents of external origin are identified and their distribution controlled;

g) prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose.

4.4.3.4 Records shall be established, documented and maintained to provide evidence of conformity to requirements and of the effective operation of the management system.

4.4.3.5 The organization shall establish, implement and maintain (a) documented procedure(s) to define the controls needed for the identification, storage, protection, retrieval, retention and disposal of records.

4.4.4 Communication

4.4.4.1 The organization shall establish, implement and maintain effective arrangements for:

a) internal communication amongst the various levels and functions of the organization;

b) receiving, recording and responding to relevant communications from interested parties.

4.4.4.2 The organization shall decide whether to actively communicate with external interested parties and shall document its decision.

4.4.4.3 If the decision is to communicate with external interested parties, the organization shall establish and implement (a) method(s) for communication.

4.5 Performance assessment

4.5.1 Monitoring and measurement

The organization shall carry out monitoring and measurement in order to determine the extent to which applicable requirements are being met. This shall include the recording of information to track performance of relevant operational controls and to evaluate conformance with the organization's objectives and the ability of the processes to achieve planned results.

4.5.2 Evaluation of compliance

The organization shall carry out periodic evaluations of compliance with legal requirements that are relevant to the scope of the management system and record the results.

4.5.3 Internal audit

4.5.3.1 The organization shall establish and maintain an audit programme for conducting periodic management system audits to determine whether or not the management system:

a) conforms to planned arrangements including the requirements of this PAS and other management system standards/specifications to which the organization subscribes (see **4.3**);

b) has been properly implemented and maintained, and is being adhered to.

4.5.3.2 The audit programme, including any schedule, shall be based on the significance of management system aspects, the organization's risks, the organization's performance and the results of previous audits.

4.5.3.3 The audit arrangements shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results.

4.5.3.4 The selection of auditors and the conduct of audits shall ensure objectivity and the impartiality of the audit process.

4.5.4 Handling of nonconformities

Where nonconformities are identified they shall be corrected and action taken to mitigate their impact (see **4.6**).

4.6 Improvement

4.6.1 General

4.6.1.1 The organization shall continually improve the effectiveness of the management system through the use of the policy, objectives, audit results, analysis of data from performance assessment, corrective and preventive actions and management review.

4.6.1.2 The organization shall define and allocate the responsibility and authority for improvement of the management system.

4.6.2 Corrective, preventive and improvement action

A process shall be established to define requirements for:

a) reviewing nonconformities or potential nonconformities (including interested parties' comments);

b) determining the causes of nonconformities or potential nonconformities;

c) evaluating the need for action to ensure that nonconformities do not occur or recur;

d) determining and implementing the appropriate action needed;

e) recording the results of action taken;

f) reviewing the effectiveness of the action taken.

Preventive and corrective actions shall be appropriate to the risks encountered.

4.7 Management review

4.7.1 General

4.7.1.1 Top management shall review the organization's management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

4.7.1.2 Reviews shall include assessing opportunities for improvement and the need for changes to the management system, including the policy and objectives.

4.7.1.3 Records of the management review shall be retained.

4.7.2 Input

The input to management review shall include, as a minimum, information on:

a) results of audits;

b) interested party feedback;

c) status of preventive and corrective actions;

d) follow-up actions from previous management reviews;

e) changing circumstances, including developments in legal and other requirements, related to the organization's aspects and associated risks;

f) recommendations for improvement;

g) data and information on the organization's performance;

h) results of the evaluation of compliance with legal and other requirements.

4.7.3 Output

The output from the management review shall include any decisions and actions related to:

a) improvement of the effectiveness of the management system;

b) improvement related to interested party requirements;

c) resource needs to enable improvement to the management system and its processes.

Annex A (informative) Guidance on the background and use of this specification

A.1 General comments

This annex is provided to assist in the understanding of why the approach specified in this PAS has been selected and to give some guidance in those areas where it is thought additional explanation is necessary. Where clauses are deemed to be self explanatory no additional guidance is provided. It is not intended to be a comprehensive guide to implementing the requirements of multiple management systems; there are many excellent sources of advice on how to implement individual management systems and integrated systems available from a number of sources.

Management system standards contain many common requirements. These common requirements are a significant proportion of those included within the standards although the terminology and specific wording or structure in which these requirements are described might vary. This PAS draws together the common requirements in management system standards and specifications and is intended to be used as a framework to implement two or more management system standards in an integrated way. In applying this high level framework for embracing the common requirements of management system standards and other management systems, it is important to recognize that there are specific requirements in individual specifications that are not included in the generic framework. Those requirements that are not common need to be addressed in addition to those in PAS 99 in order to meet the specific standards/specifications to which the organization subscribes.

The model used for the framework relates closely to the common elements proposed in ISO Guide 72 [1] which is a guide for standards writers. Guide 72 included a framework which was developed as a model for enabling writers to produce standards that covered the various core elements in a consistent manner. This would then enable organizations to integrate their systems to the extent that was appropriate to the needs of the organization.

The writers of this PAS considered that this was the most appropriate framework for this specification as it enables the existing standards and specifications given in the scope to be accommodated and enable effective and efficient management of the common management system requirements.

A.2 Process approach

ISO 9001 uses the process approach for identifying those areas that need to be controlled in order to deliver an efficient and effective product or service. There is no such requirement in some of the other standards/specifications but this approach can be usefully employed to identify all the issues an organization needs to manage and then to identify those aspects that need to be controlled because in the absence of effective control there would be a risk to some interested party.

Often the word “procedure” is used in management system standards/ specifications and there can be confusion as to what a procedure is and how it relates to a process. In simple terms, a process is an activity, and a procedure is the formalization of the process stating how the process should be performed, which may be documented.

A.3 Risks, aspects and impacts

At the heart of modern management standards is the ‘‘risk based approach’’. This can be recognized from the definition of management system in combination with the definition of risk. A management system assists an organization in establishing policies and achieving objectives. Risks are possible occurrences that could impact upon objectives. Thus, it is logical that management systems are there to manage risks in order to achieve objectives. In some disciplines the risk based approach is closely related to legal requirements (safety for example) which obviously have to be satisfied. ISO 9001 is at first sight less explicit in its risk based approach because there is no general requirement to identify and assess critical characteristics related to quality. However, customer and regulatory requirements need to be identified and form the basis for the assessment, control and monitoring of the organization's processes to ensure these requirements are met. Many organizations apply such techniques as FMEA (Failure Modes and Effects Analysis) within their quality system to embrace the risk approach. The requirement to assess risks is the principal driver for occupational health and safety, information security and food safety management systems and is likely to feature in all future management system standards.

In this PAS, the term “aspect” is used to identify those issues where control might be required because they pose a risk (positive or negative). It will become apparent that there are many aspects with respect to information security, quality, environment, safety etc. that can have an impact on an organization. It would not be sensible for an organization to try and tackle all these at once. The approach recommended is one where the organization identifies those that could have the most **significant impact** and need to be controlled and/or reduced through improvement programmes.

A.4 Specific Guidance

The following clauses give guidance where it is thought the text of the specification might need some further amplification. Where the text is thought to be explicit enough and is adequately covered in the various standards/specifications that will be adopted or implemented by the users of this PAS, no further guidance is given.

As explained in the main text of this PAS, for each management system standard/specification, common requirements may be identified as follows:

A.4.1 Management system requirements (see 4.1)

No additional guidance is necessary apart from that provided in the introductory sections of this annex.

A.4.2 Guidance on management system policy (see 4.2)

It is clearly sensible to define what one intends to do before starting to do it, and that is the basis of a policy statement. Each management system standard goes on to specify certain things that the policy statement should include.

The wording is based on ISO 9001, but is of general application; it may be used to cover other specific elements, such as industry codes of practice.

Issues to be covered include a policy to demonstrate the organization's commitment to meeting the requirements related to the management system and to establish an overall sense of direction and principles for action. It should also provide a framework for setting objectives.

A corresponding requirement can easily be identified in any management system standard. For example, ISO 9001 requires ''documented statements of a quality policy…'' and ISO 14001 requires that ''Top management shall define the organization's environmental policy…'' and that this includes a commitment to prevent pollution. The organization may decide to have separate policies for each discipline, or an integrated policy provided that this covers the requirements of each individual standard.

A.4.3 Guidance on planning (see 4.3)

A.4.3.1 General

There is a need to identify what the management system is intended to support, what is to be done, by whom, how and when, and what resources will be needed. Above all there will need to be a commitment by management at all levels to the development of the system. Training will be needed for people to be able to operate the system and also to enable key employees to take part in its development in identifying hazards and opportunities and assessing the risks. The programme of implementation can in itself be a valuable aid to making all employees aware of the principles of risk and risk management as well as the specifics of safety, quality, etc.

Having defined the policy stating what is intended, the next logical step is to plan how it is to be put into practice. The framework lists the following subjects which should be covered:

a) Identification and evaluation of aspects, impacts and risks (see **4.3.1**);

b) Identification of legal and other requirements (see **4.3.2**);

c) Contingency planning (see **4.3.3**);

d) Objectives (see **4.3.4**);

e) Identification of organizational structure, roles, responsibilities and authorities (see **4.3.5**).

Contingency planning (see **4.3.3**) should be extended to cover specifically disaster recovery and business continuity.

In any sizeable organization the process of implementing a management system will be a large one, involving many people and considerable time; benefits might be gained from using a formal project management approach to implementation.

Many organizations will already have some formal control of their processes and the management system might already be process based. Those who are embarking on the route to integration might well find the approach suggested in PAS 99 a convenient way to work although it is not the only way.

If the process approach is to be adopted, the initial step should be to identify the processes and sub-processes involved in the organization. If the organization has adopted ISO 9001 this will have been done already, at least for those processes which affect the quality of the output. If the processes are mapped and the map is published throughout an organization, it can be invaluable in demonstrating to employees how they contribute to the objectives.

For each process the following tasks should be carried out:

a) Identification of the inputs and outputs;

b) Identification of the aspects and impacts associated with the process;

NOTE This should be done by those people actually engaged in the process, suitably trained and assisted by managers, as necessary.

c) Identification of those aspects that could have a significant impact, and prioritizing them;

d) Deciding on control measures and implementing them.

For each process the aspects need to be identified which could have an impact on each of the management areas that are to be brought within the overall management system. For example:

a) In the input stage, is there anything that might significantly affect:
   - the quality of the output?
   - the environment?
   - the occupational health and safety of the employees or those affected by the organization's activities?

b) In the output stage, is there anything that might significantly affect:
   - the quality of the output?
   - the environment?
   - occupational health and safety?

This approach demonstrates one of the advantages of an integrated system. In a traditional system these questions would be considered separately, at different times and quite possibly by different groups of people. In an integrated system, all these aspects (and others, such as customer satisfaction or information security) can be considered at the same time by the people who are actually involved in the process. There is, however, no requirement to have an integrated approach to identifying and prioritizing aspects. The simple approach described above is offered only as an example of what might be adopted. However, by approaching it in the above manner, the chance of conflict from addressing one issue without considering the impact on the other issues can be reduced.

A.4.3.2 Identification and evaluation of aspects, impacts and risks (see 4.3.1)

Those aspects which carry a high risk will be managed first. There are many ways of assessing risk, but a simple system is often the best. Elaborate systems usually add very little in practice. Even organizations that operate in high risk sectors have found an approach based on that proposed can be useful as a first step. They then use more sophisticated methods such as Hazard Analysis and Operability Studies (HAZOPS) with those risks that are identified as posing the greatest risk to the organization and its interested parties.

All of the significant aspects should be subject to some form of control from the management system. In addition, the most significant aspects should also be the subject of improvement programmes to help the organization to reduce its risks.

For each process the questions are:

a) What (aspect) could go wrong?

b) What would the effect (impact) be if it did go wrong?

c) How likely is it to happen?

The answers in combination give a measure of risk, as illustrated by the following matrix. If an event is quite likely and the effect would be serious, then the risk is high and something needs to be done about it straight away – possibly stop the process or even evacuate the factory. If the risk is moderate, something still needs to be done but not with the same degree of urgency. If the event is improbable and the impact insignificant, then the risk is one that the organization will probably feel that it can live with.

	Very improbable	**Not probable**	**Rarely occurring**	**From time to time**	**Fairly regularly**
No effect					
Negligible effect					
Slight effect					
Considerable effect					
Great effect					
Very great effect					

white: tolerable risk
shaded: high risk, risk controls needed
black: very high risk, risk-reducing actions are necessary

This approach can be used to identify the stage in the process that could have the greatest impact on the quality of the product or customer satisfaction. It is the most significant impacts that should be addressed in the first instance. Those risks that are thought to be tolerable will have little impact on the organization and in the hierarchy of managing aspects may not need to be dealt with at all unless the organization recognizes some benefit.

A.4.3.3 Identification of legal and other requirements (see 4.3.2)

No additional guidance is necessary.

A.4.3.4 Contingency planning (see 4.3.3)

As part of its risk management programme the organization needs to consider its response to any emergency that might arise. This should include disaster management.

For instance, ISO 9001 clause **8.3** deals with product recall as this can be an issue any well managed manufacturing organization would have established arrangements for. Similarly, any fire or emergency that would cause business interruption should have been addressed.

Accordingly, there is a whole spectrum of possible events which might arise which would affect the ability of the organization to continue. This will range from the failure of a major customer (or supplier) to a fire or flood or even an earthquake. Every day such an event happens somewhere in the world, and if the event has not even been considered by the management of the organization concerned its prospects for survival will be poor.

A.4.3.5 Objectives (see 4.3.4)

It is up to the management of the organization to decide how the objectives are to be selected and ranked. The objectives chosen should be relevant and realistically achievable taking into account the resources available. If employees have been involved in identifying the key aspects it is likely that they will also be able to contribute to defining key objectives. The objectives should be positive and meaningful. An objective such as ''to reduce waste'' is too general to be constructive. ''To reduce waste by x% over a period of y months'' is better so long as the present level of waste is known and there are effective means of measuring it. Often, identifying a key objective will reveal a number of subsidiary objectives which have to be attained first, and conflicts might arise over the use of limited resources. Accordingly, the selection of objectives needs to be done with care.

In ISO 14001, there is the term "target" as well as "objectives". A target is seen as being lower level objective (it might be for instance the timescale in which it hopes to achieve an objective). A target is a statement of what an organization hopes may be achieved but is not critical to its future. If the organization fails to meet its targets it may need to review its objectives.

A.4.3.6 Organizational structure, roles, responsibilities and authorities (see 4.3.5)

The successful implementation of a management system (MS) will depend on the commitment of top management. The MS needs a top manager as its focus who shows commitment and enthusiasm and who can convey this enthusiasm to all the employees involved. There also needs to be someone appointed who will be responsible for the implementation and operation of the MS.

The increasing awareness of the importance of risk management will help as the management system should be the cornerstone of the risk control measures of the organization. It is vital that every manager and every employee understand their roles in the implementation of the system. The competencies required for each task need to be identified, and training provided where necessary. There needs to be a progress reporting system, and each manager should have a specific programme of phases in achievement.

A.4.4 Guidance on implementation and operation (see 4.4)

A.4.4.1 Operational control (see 4.4.1)

This term does not appear in ISO 9001, but there are clauses in ISO 9001 that relate to this requirement in PAS 99. In particular, requirements to ensure that the product is controlled are apparent in ISO 9001 clauses **6.4** (Work environment), **7.1** (b and c) (Planning of product realization), **7.5.1** (Control of production and service provision) and **7.5.2** (Validation of processes for production and service provision).

A.4.4.2 Management of resources (see 4.4.2)

No additional guidance is necessary.

A.4.4.3 Documentation requirements (see 4.4.3)

No additional guidance is necessary.

A.4.4.4 Communication (see 4.4.4)

Communication from management to employees should be appropriate so that they can carry out the desired tasks in terms of the relevant systems and understand the reasons why. There needs to be a corresponding and efficient system of communication in the opposite direction from the employee to management at all levels. Remember that the workforce is always an interested party that may act through external bodies such as trade unions, and furthermore is the best source of information on aspects and risks in the workplace.

It should be recognized that the method of communication and language used should be appropriate to the needs of the workforce and be in such a form that they can easily understand the information being provided to them.

The arrangements with suppliers and contractors may need to be more formalized than previously to meet this requirement.

A.4.5 Guidance on performance assessment (see 4.5)

Having installed the system and got it working, the next requirement is to see how it is performing. This will include:

a) Monitoring and measurement (see **4.5.1**);

b) Evaluation of compliance (see **4.5.2**);

c) Management of internal audits (see **4.5.3**);

d) Handling of nonconformities (see **4.5.4**).

A.4.5.1 Monitoring and measurement (see 4.5.1)

Monitoring and measurement are essential in order to make sure that the system is operating as intended and as the basis for demonstrating continual improvement.

The system should be implemented so that performance can be readily evaluated. Monitoring must be both proactive (in achieving the plans and objectives) and reactive, such as responding to and reporting on reportable accidents or major incidents.

A.4.5.2 Evaluation of compliance (see 4.5.2)

No additional guidance is necessary.

A.4.5.3 Management of system audit (see 4.5.3)

Audits are essential to ascertain whether the system is being followed in all respects, and if not, why not. They are a requirement of every management system standard. Deficiencies might be identified in staff or in the system itself. Audits are often regarded as a necessary chore but more properly they should be recognized as providing opportunities for improving the system.

In the case of PAS 99, it should be recognized there can be many benefits of an integrated audit. Those areas which are common need only be assessed once instead of two or three times depending on how many standard system requirements have been adopted. The specific requirements will obviously need to be addressed and then specialist skills might be needed. It may be beneficial for instance, depending on the complexity of the organizations and its risks, that a multi-disciplined audit team is used. There will need to be personnel with expertise in auditing the core management system and specialists for evaluating the control of those aspects that should be controlled within the requirements of the specifications to which the organization subscribes. A food hygienist may well be needed for ISO 22000 for example.

A.4.5.4 Handling of nonconformities (see 4.5.4)

No additional guidance is necessary.

A.4.6 Improvement (see 4.6)

No additional guidance is necessary.

A.4.7 Management review (see 4.7)

No additional guidance is necessary.

Annex B (informative) Common requirements

Common requirements of quality, environmental management and health and safety management

Requirements of PAS 99	ISO 9001 Quality clause	ISO 14001 Environmental management clause	OHSAS 18001 Health and safety clause
4.1 General requirements	4.1	4.1	4.1
4.2 Management system policy	5.1, 5.3	4.2	4.2
4.3 Planning		4.3	4.3
4.3.1 Identification and evaluation of aspects, impacts and risks	5.2, 5.4.2, 7.2.1, 7.2.2	4.3.1	4.3.1
4.3.2 Identification of legal and other requirements	5.3(b). 7.2.1(c)	4.3.2	4.3.2
4.3.3 Contingency planning	8.3	4.4.7	4.4.7
4.3.4 Objectives	5.4.1	4.3.3	4.3.3
4.3.5 Organizational structure, roles, responsibilities and authorities	5.5	4.4.1	4.4.1
4.4 Implementation and operation			
4.4.1 Operational control	7	4.4.6	4.4.6
4.4.2 Management of resources	6	4.4.1, 4.4.2	4.4.1, 4.4.2
4.4.3 Documentation requirements	4.2	4.4.4, 4.4.5, 4.5.4	4.4.4, 4.4.5, 4.5.3
4.4.4 Communication	5.5.3, 7.2.3, 5.3(d), 5.5.1	4.4.3	4.4.3
4.5 Performance assessment			
4.5.1 Monitoring and measurement	8.1	4.5.1	4.5.1
4.5.2 Evaluation of compliance	8.2.4	4.5.2	4.5.1
4.5.3 Internal audit	8.2.2	4.5.5	4.5.4
4.5.4 Handling of nonconformities	8.3	4.5.3	4.5.2
4.6 Improvement			
4.6.1 General	8.5.1	4.5.3	4.5.2
4.6.2 Corrective, preventive and improvement action	8.5.2, 8.5.3	4.5.3	4.5.2
4.7 Management Review			
4.7.1 General	5.6.1	4.6	4.6
4.7.2 Input	5.6.2		
4.7.3 Output	5.6.3		

Common requirements of information technology, security systems and food safety

Requirements of PAS 99	**ISO/IEC 20000 IT Service management Specification clause**	**ISO/IEC 27001 Information Security clause**	**ISO 22000 Food Safety clause**
4.1 General requirements	3	4.1, 4.2	4.1
4.2 Management system policy	3.1, 4.4.1	5.1	5.1, 5.2
4.3 Planning	4.1	4.2	5.3
4.3.1 Identification and evaluation of aspects, impacts and risks	4.1(f), 4.2(d)	4.2	5.3, 7.1, 7.2, 7.3, 7.4
4.3.2 Identification of legal and other requirements		4.2.1 (b2)	7.2.3
4.3.3 Contingency planning	8.2		3.3, 5.7, 7.10, 7.10.4
4.3.4 Objectives	4.1(b), 5.0	4.2.2	7.5, 7.6
4.3.5 Organizational structure, roles, responsibilities and authorities	4.2	4.2.2	5
4.4 Implementation and operation			
4.4.1 Operational control	4.2, 6.0	4.2.2	7.7, 7.8, 7.9
4.4.2 Management of resources	3.1, 3.3	5.2.1, 5.2.2	5.1, 5.3, 5.4, 5.5, 6.1, 6.2
4.4.3 Documentation requirements	3.2	4.3	4.2
4.4.4 Communication	3.1(b), 7	4.2.4(c)	5.6
4.5 Performance assessment			
4.5.1 Monitoring and measurement	4.3	4.2.3	7.6.4, 7.6.5, 8.3
4.5.2 Evaluation of compliance	4.3	4.2.3	8.4.3
4.5.3 Internal audit	4.3	6	8.4.1
4.5.4 Handling of nonconformities	4.3	4.2.4	7.6.5, 7.10
4.6 Improvement			
4.6.1 General	4.4	4.2.4, 8.1	8.1, 8.5
4.6.2 Corrective, preventive and improvement action	4.2.4(b), 8.2, 8.3	8.2, 8.3	8.2
4.7 Management Review			
4.7.1 General	3.1(g)	7.1	5.8, 8.5.2
4.7.2 Input		7.2	5.8.2
4.7.3 Output		7.3	5.8.3

Bibliography

Standards publications

BS EN ISO 9000:2000, *Quality Management Systems – Fundamentals and vocabulary*

BS EN ISO 9001:2000, *Quality Management Systems – Requirements*

BS EN ISO 14001:2004, *Environmental Management Systems – Requirements with guidance for use*

BS EN ISO 22000:2005, *Food safety management systems – Requirements for any organization in the food chain*

BS ISO/IEC 20000-1:2005, *Information Technology service management*

BS ISO/IEC 27001:2005, BS 7799-2:2005, *Information Technology – Security techniques*, *Information Security management systems – Requirements*

BS 8800:2004, *Guide to occupational health & safety management systems*

OHSAS 18001:1999, *Occupational Health & Safety Management Systems – Specification*

Other publications

[1] ISO Guide 72:2001, Guidelines for the justification and development of management system standards

Further reading

Creating a Manual, IMS Risk Solutions, London: BSI, 2003

HINCH, H. *IMS: Managing Food Safety,* London: BSI, 2003

Integrated Management systems – Good practices and experience feedback AC X 50-200 AFNOR

ISO Guide 73:2003, Risk management – Vocabulary – Guideline for use in standards

MURRAY, P. *IMS: Information Security,* London: BSI, 2003

SMITH, D. *IMS: The Framework*, London: BSI, 2001

SMITH, D. *IMS: Implementing and Operating*, London: BSI, 2002

This page deliberately left blank

BSI – British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.
Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001.
Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111.
Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002.
Fax: +44 (0)20 8996 7001. Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

389 Chiswick High Road
London
W4 4AL