32 International EHS Auditing Standards

The International Organisation for Standardisation is a federation of national standards organisations that agrees and specifies international standards in a wide range of applications. In this chapter, we will summarise the quality, environmental and safety management standards and their interrelationships.

The basis for these standards are the range of quality standards, of which the key one is ISO 9001 ('Quality Management Systems Requirements'). This standard, approved in 2015, adopts the 'plan–do–check–act' approach proposed by W. Edward Deming.

In the model shown in Figure 32.1, the four stages in the model relate to how the management system and processes are applied and implemented. An interpretation of the four stages in the model is

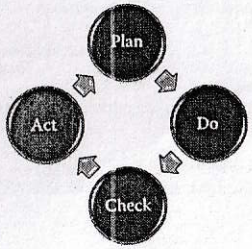

FIGURE 32.1 The PDCA model.

1. Plan: Establish the objectives and processes required to achieve the results in accordance with the organisations stated policy.
2. Do: Implement the process.
3. Check (the auditing stage): Monitor and measure the processes against the objectives set.
4. Act: Take continual improvement action.

This plan–do–check–act approach is the principle behind all three of the key ISO standards that apply to safety, health and environmental management. The circuit of using audits to identify corrective actions, which when resolved lead to improvements, then results in a never-ending upwards spiral of improvement. The application of quality management techniques to environmental, health and safety management

is entirely logical, as it advocates treating the prevention of all types of harm in the same way as other aspects of managing an organisation. Why then is it necessary to have separate standards on quality, environmental management and safety, when they could all be integrated under a single quality standard? The cynics might argue that corporate registration under international standards is big business and income for the national standards bodies and their associates, and there are particular companies that successfully use the ISO 9001 quality management approach across all aspects of management, including safety, health and environmental management. It is also quite common now to find organisations integrating their environmental, health, safety and quality organisations because of the similarities in management styles.

The answer to the question is partly historical and partly to do with the way in which the quality standard is presently structured. ISO 9001 was the first of the internationally agreed standards relating to quality management. Because it is generally applicable, it needs to be relevant to a very wide range of organisations as diverse as local government, hospitals, haulage companies, financial institutions and nuclear power plants. Consequently, the standard requires organisations to establish for themselves what criteria it is important for them to meet. In the early days of the introduction of the standard, some organisations were setting very demanding requirements for themselves, while others set much less demanding ones. It led at that time to a belief that if the requirements were easy to achieve, then getting certification against ISO 9001 was not too difficult, and some felt that this gave a misleading result. There was a feeling that for some organisations, it encouraged the setting of low standards and resulted in the quality threshold being low.

The desire to apply a quality approach to environmental management opened up a new opportunity. Unlike business objectives, environmental objectives are relatively clear, in that virtually everyone lives and works in an environment surrounded by air, ground or water. The consequences of contaminating any one or more of these three aspects of the environment are well understood, and although the types of contaminants are myriad, the solutions are quite limited. This offered the opportunity for the international standard on environmental management (ISO 14001) to be much more focused and include some specified objectives. The application of ISO 14001 resulted in much less variability in authorisations, and its success has lead to a similar approach being taken to the quality management of safety in the international standard OHSAS 18001.

The use of similar approaches in the application of international quality, environmental and safety standards means that the same style of Level 1 (compliance) auditing can be universally applied. The benefit of this to the organisation is that the same auditors, auditor training, audit planning and corrective action tracking system can in theory be applied to quality, safety and environmental requirements. This has the potential to result in more competent auditors, better auditee understanding of the benefits of auditing and a single streamlined process for dealing with nonconformity and noncompliances. Most importantly, it emphasises that environmental, health and safety management is not a separate independent strand of the management process but is fully integrated within it.

A SUMMARY OF ISO 14001 REQUIREMENTS

Background

This standard aims to achieve a balance between what it describes as the three pillars of sustainability, which are the environment, society and the economy (Figure 32.2).

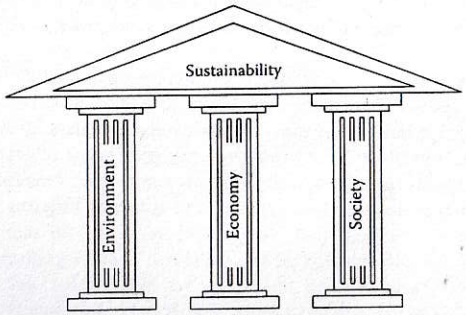

FIGURE 32.2 The three pillars of sustainability.

ISO 14001:2015 aims to provide a systematic approach to environmental management. It differs from ISO 9001 in that it does not just provide for compliance with an organisation's own standards, it also defines those areas of environmental management that are important. The standard is intended to help organisations to

- Improve environmental performance
- Achieve regulatory compliance
- Achieve the organisation's environmental objectives
- Encourage a 'life cycle' approach to the way in which products and services are produced, used and disposed of

The standard requires that the organisation has an environmental management system to control those aspects of their operation that can have potential impact on the environment. In this respect, the environment is defined as the 'surroundings in which the organisation operates, including air, water, land, natural resources, flora, fauna, humans and their interrelationships'.

To conform to the standard, the organisation has to demonstrate conformance to detailed requirements under the following categories:

1. Environmental Leadership and Commitment
2. Environmental Policy
3. Organisational Roles and Responsibilities
4. Planning
5. Support (Resources/Competence/Awareness/Communication/Information)
6. Operation

7. Environmental Performance Evaluation
8. Internal Auditing
9. Management Review

In preparing for an environmental management system, the management team must identify who the interested parties are and their requirements. This will aid the organisation in identifying for itself its environmental policy and which requirements should become its environmental objectives. In large organisations, these objectives may be tiered so that the objectives of each individual facility contribute to the achievement of the organisation's overall strategic objective.

In order to implement the environmental policy, the organisation should follow the four steps of the plan–do–check–act model described earlier. Planning requires the establishment of an environmental management system. As with any management system, an environmental management system will not exist and thrive without management's leadership and commitment.

Category 1: Leadership and Commitment

It is essential that senior management demonstrate commitment to the environmental management system through their actions. This begins by establishing the environmental policy and then demonstrating active support in the implementation of that policy by

- Setting good personal examples
- Integrating environmental objectives with the organisation's strategic direction
- Providing adequate human and financial resources
- Monitoring and adapting the systems to ensure that environmental objectives are met

A starting point for any Level 2 or Level 3 audit should always be for the senior auditor to establish the extent of senior management commitment, where the individuals concerned will be expected to demonstrate those responsibilities that they are personally accountable for.

Category 2: Environmental Policy

Senior management are responsible for the preparation and issue of the environmental policy and for communicating that policy to those affected by it. The organisation must ensure that its environmental objectives are consistent with its policy. The policy should be periodically reviewed and updated in light of relevant changes and, in particular, should be approved by the current most senior manager for the organisation or that part of the organisation.

It is important that the policy addresses commitments to the protection of the environment and the principle of 'pollution prevention'. The policy should encapsulate all those potential areas where the organisation's activities can have either a positive or negative impact on the environment.

The four principles that should be covered in the environmental policy are

1. To protect the environment
2. To comply with regulatory requirements
3. To meet the organisation's environmental objectives
4. Continuous improvement

Category 3: Organisational Roles and Responsibilities

Senior management must allocate roles and responsibilities throughout the organisation for the implementation and ongoing management of the environmental management system. This may mean the appointment of a suitably qualified and trained 'environmental manager', but more importantly, it will require the assigning of responsibilities throughout the management line and ensuring that those people at the 'shop floor' level where environmental impacts are most likely to arise are also trained and aware of the importance of their individual roles and duties.

There must be clear internal accountability for ensuring that the environmental management system conforms to ISO 14001 and that such conformity is maintained by rigorous checking in the form of Level 1 compliance audits.

The organisation must decide what environmental parameters are relevant for monitoring improvement and shall then appoint responsibilities for the gathering, analysing and reporting of that information on a regular frequency.

Category 4: Planning

The organisation must consider what parts of its operations, products or services can have an effect on the environment either at a local, regional or global level. Such parts of the operation are known as 'environmental aspects'. In identifying these environmental aspects, the organisation is required to consider not only the normal smooth running state of the operation but also

- Abnormal conditions
- Reasonably foreseeable emergencies
- New developments/products or services

The organisation must maintain documentary records of the criteria it used to identify environmental aspects and which of those it considers to be significant.

There should be a register of applicable environmental legislation kept up to date with clear accountabilities relating to the compliance assurance of each legal requirement. In addition to national legislation, there may be local binding agreements, industry sector agreements, corporate objectives or other nonnegotiable environmental obligations that need to be included when identifying which environmental aspects are significant.

The organisation must plan to address the significant environmental aspects and corrective actions to ensure compliance with regulation. It is normal that these environmental improvement plans will look forward several years into the future, as it is recognised that some environmental improvements may incur substantial capital

expenditure, which requires long-term forward planning. Ideally, these plans are on a rolling basis, so that as some actions are completed, new actions are added. The plans should clearly identify who should do what and by when. Once the environmental management systems are established, the maintenance of the system is checked via the Level 1 auditing system. In order to ensure elements of the system do not get overlooked, a rolling audit schedule should be established along the lines discussed in Chapter 6 (Figure 6.1).

Category 5: Support

The organisation must decide how it will resource the establishment, implementation, maintenance and ongoing improvement of the environmental management system. To do this, the management team will need to consider financial, human, equipment and information technology (IT) resources. There is always an initial financial cost implication, even if the management system relies entirely on existing people, as there will be training, communication, systems familiarisation and debugging and new auditing commitments, all of which will take time and money. It is important that this initial cost implication is understood, as the management team's credibility will be undermined if they announce a plan to gain accreditation to ISO 14001 and then abandon it part way down the track because they don't have the resources. It should be recognised that once the system is fully implemented, there are often financial rewards because costly environmental incidents and prosecutions are avoided and often raw material and services consumption is reduced.

It is important to ensure that responsibilities are assigned to competent people, and so training and competence validation will need to be demonstrated.

A key part of any successful management system is two-way communication, and this is no different in the case of the environmental management system. The organisation must have effective internal systems to identify what it is going to communicate, to whom and when, and this information must be recorded. Most organisations have some sort of regular communication sessions that cascade throughout the organisation, and it is usual to integrate the environmental communications into these existing channels rather than create separate and parallel systems. What does not always exist is an effective means of communicating to external stakeholders, and the implementation of ISO 14001 will ensure that appropriate arrangements are made.

In common with ISO 9001, ISO 14001 requires that procedural documents are produced in a standardised format and that there is a document control process in place to authorise and issue changes.

Category 6: Operation

The organisation must have processes in place to meet the objectives set for the environmental management system. Controlling these processes may be implemented using the 'hierarchy of controls' (Figure 32.3), which in the case of ISO 14001 identifies that the elimination of the environmental risk is the best risk control option, followed by substitution by a lesser risk, and those are preferable to administrative controls, which can be subject to human error.

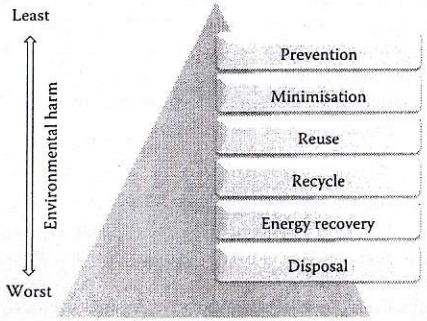

FIGURE 32.3 Environmental hierarchy.

Outsourced processes such as waste recycling and disposal also have to be effectively controlled and those controls demonstrated. These outsourced operations will need to be checked by specialist Level 2 audits to demonstrate that the controls are effective. Where outsourcing involves the use of contracted services, those contracts need to reflect the appropriate environmental objectives.

A key part of operational requirements is the need for emergency response plans, which will mitigate adverse environmental impacts from emergency situations. These situations are not just limited to environmentally related incidents but also where, for example, in fire situations there can be the release of airborne toxins such as asbestos or the escape of large quantities of contaminated firefighting water. Foreseeable emergencies should take account of severe weather and relevant product transport emergencies.

Affected personnel must be trained in the emergency action requirements, and emergency control plans must be subject to periodic testing and review.

Category 7: Environmental Performance Evaluation

Where emission monitoring and analysis is essential for effective environmental control, that monitoring equipment must be suitable and calibrated or verified as required to ensure its reliability. Records of previous monitoring must be maintained as proof of ongoing measurement, evaluation, analysis and corrective action. The checking of calibration records is a key part of the auditor's verification tasks.

Category 8: Internal Auditing

The organisation is required to provide assurance of compliance with the requirements of ISO 14001. This is done by Level 1 (compliance-level) auditing and then taking corrective action where required. An audit programme is required, and audit frequency will depend on the criticality of that aspect of the management system in prevention of pollution or harm. Local auditors need to be trained and competent, and the results of the audit must be reported and actioned by management. Documented evidence that audits have been conducted need to be maintained.

Category 9: Management Review

Senior management must periodically undertake a review of the environmental management system to ensure its suitability and effectiveness, taking into account relevant internal and external changes and the appropriateness of current resources. The review must consider the records of

- Environmental monitoring
- Nonconformities
- Corrective actions
- Audit results

Documentary records must be maintained relating to the management review.

Certification to ISO standards (previously known as 'accreditation') is carried out by a very limited number of approved certification bodies who are authorised by ISO via the local national standards bodies. It is not possible for organisations to officially self-certify conformity with the ISO standards.

A SUMMARY OF OHSAS 18001 REQUIREMENTS

At the time of writing, the Occupational Health and Safety Assessment Series standard 18001 (OHSAS 18001:2007) is the current international standard identifying requirements for occupational health and safety management systems. This standard is scheduled to be replaced in early 2018 with ISO 45001.

OHSAS 18001 was developed to compliment ISO 9001 (quality) and ISO 14001 (environmental) in response to the demand for an internationally accredited system for occupational health and safety management. The early version was launched as a specification rather than a standard, hence its designation 'OHSAS' rather than 'ISO'. The 2007 version became described as a 'standard' and the migration to ISO 45001 will complete this process making the document fully compatible with ISO 9001 and 14001.

In common with the International Quality and Environmental Management Standards, OHSAS 18001 adopts the plan–do–check–act model described earlier, but the traditional way of portraying this to demonstrate never-ending improvement is shown in Figure 32.4.

The standard is written with the intention of being auditable, with this leading to the opportunity for formal accreditation of the organisation's occupational health and safety management system.

The current standard structure differs slightly from that in ISO 14001, but in principle it covers all the same topics. The OHSAS 18001 management system requirements are

- Occupational health and safety policy
- Planning
- Implementation
- Operation
- Communication

- Documentary control
- Checking
- Management review

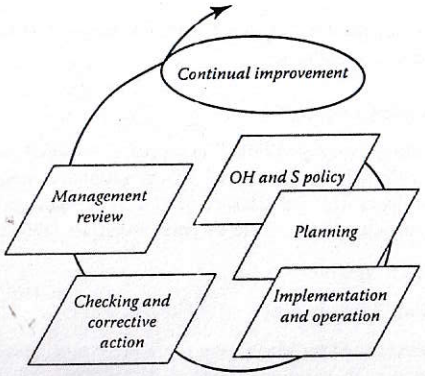

FIGURE 32.4 The OHSAS 18001 management system model. (Permission to reproduce extracts from British Standards is granted by BSI Standards Limited (BSI). No other use of this material is permitted. British Standards can be obtained in PDF or hard-copy formats from the BSI online shop: https://shop.bsigroup.com.)

Category 1: Occupational Health and Safety Policy

In many westernised countries it is now a legal requirement for organisations to have an occupational health and safety policy. For the purposes of OHSAS 18001, this policy should be suitable for the type and scale of risk that exists within the organisation's operations. The policy should be periodically reviewed and updated in the light of relevant changes, and in particular, should be approved by the current most senior manager for the organisation or part of the organisation. The policy should be communicated to all those who are affected by it.

In a similar way to ISO 14001, the four principles of commitment that should be covered in the occupational health and safety policy are

1. To aim to prevent injury and work-related ill health
2. To comply with regulatory requirements
3. To meet the organisation's occupational health and safety objectives
4. Continual improvement in the management of occupational health and safety

Category 2: Planning

The organisation must have formal arrangements in place for the ongoing identification of hazards and the consequential assessment of risks. Residual risks must be effectively controlled. These procedures should take into account everyone who can

be affected by the work activity, including contractors and visitors. The risk assessment shall be proactive rather than reactive and must include

- Human factors, such as behaviour, capability and ergonomics
- Routine and non-routine tasks
- Hazards created both within the workplace and arising from or affecting adjacent work activities
- Equipment and materials at the workplace
- The design of workplaces and equipment therein

The resulting assessment must identify and prioritise risk, and where the risk is unacceptable, identify what controls are necessary to deal with the residual risk. When determining what controls are appropriate, the hierarchy of controls should be applied as shown in Figure 32.5. Control options higher up the hierarchy are considered to be more effective than those lower down.

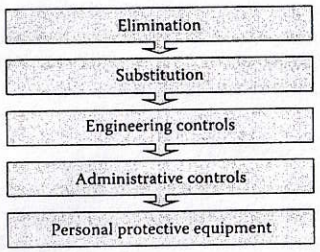

FIGURE 32.5 OHSAS 18001 'hierarchy of controls'.

The results of these risk assessments must be recorded and communicated to those affected.

As with ISO 14001, a register of applicable health and safety legislation should be maintained, with clear accountabilities relating to the compliance assurance of each statutory obligation. In addition to national legislation, there may be local binding agreements, industry sector agreements, corporate objectives or other nonnegotiable occupational health and safety obligations that need to be complied with, and elements of all these requirements may form part of the organisation's occupational health and safety objectives. These objectives must be measurable.

Category 3: Legal Compliance

The organisation must have arrangements in place to clearly identify what current laws and regulations are applicable to their operations and must ensure that these statutory obligations are taken into account in the health and safety management system, including procedures, instructions and other forms of risk control, such as guards, signs and protective equipment and so on. This information must be kept up to date.

Category 4: Objectives

The organisation must set, implement and maintain a set of written health and safety objectives and these must be in keeping with both the health and safety policy and local legislation. Performance against these objectives must be monitored. An ongoing health and safety improvement plan must identify what actions are required to achieve the objectives and who is responsible for delivering that improvement and by when.

Category 5: Roles and Resources

The senior management team are responsible for health and safety at the facility and for the health and safety management system. They are responsible for ensuring that suitable and sufficient resources are provided to allow the organisation to achieve its health and safety objectives. In order to do this, the management team must define the roles and responsibilities relating to effective health and safety management throughout the organisation. A specific member of the local senior management team must be appointed with specific responsibility for health and safety. This appointment must be communicated to all people working within the organisation.

Category 6: Training and Competence

All persons working within the facility must be educated, trained and sufficiently experienced to do their job safely and without harm to their health. In order to achieve this, the organisation must carry out an assessment of training requirements and then provide suitable training to satisfy these requirements. All persons, including employees, contractors and visitors must be informed of the hazards and risks associated with their work activities and what their own personal responsibilities may be to protect their own safety. This information should be in a form that is appropriate for the individual concerned and should take into account such things as literacy and language skills. It must be made clear to all persons carrying out work at the facility what will be the consequences of not conforming to the organisation's health and safety procedures.

Category 7: Consultation

In addition to the requirements to communicate hazards and risks, there is a requirement under the standard to ensure that workers are consulted in important decisions relating to their health and safety. This may apply to their participation in hazard identification, risk assessment, specification and choice of workplace controls and their involvement in relevant accident and incident investigations.

Category 8: Documentation

As with all ISO standards, OHSAS 18001 is required to have certain basic documentation, which includes

- Health and safety policy and associated objectives

- The scope of the health and safety management system
- Associated records (those required to ensure the system is maintained)

There must also be a document management system to ensure that both distribution and updating is effectively controlled.

Category 9: Operational Control

Control of health and safety is not just linked to workers' activities. Management controls need to be established over purchased goods, substances and services to ensure that hazards are identified and risks controlled. The management system should cover not only the controlling of acts by persons but also the consequences of human omissions.

Category 10: Emergency Preparedness

A procedure must be established for identifying foreseeable emergencies and then arrangements for dealing with those emergencies. Emergency response actions should take account of the requirements of neighbours and the emergency services. The emergency procedures must be periodically tested in order to ensure personnel are trained and lessons are learned.

A system designed to assist small and medium-sized enterprises in complying with the OHSAS 18001 requirement is the SHEEMS system, as shown in Figure 32.6 (more information at www.solwayconsulting.com).

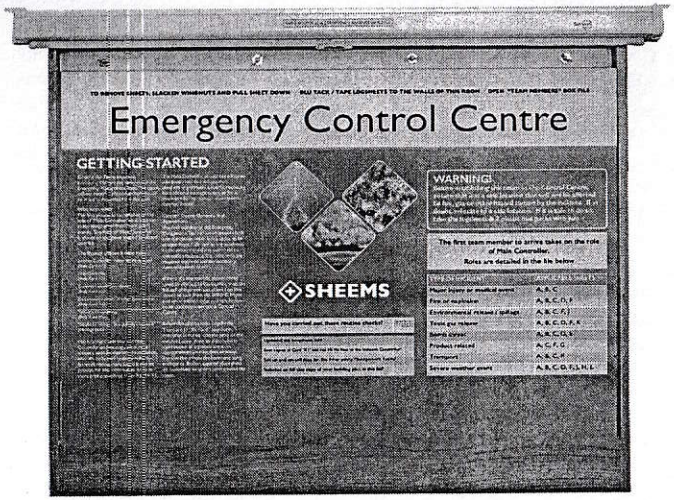

FIGURE 32.6 System for small and medium-sized enterprises that need to comply with the emergency management requirements of OHSAS 18001/ISO 45001.

Category 11: Checking (Monitoring and Auditing)

The organisation is required to provide assurance of compliance with the requirements of OHSAS 18001. This should be done by Level 1 (compliance-level) auditing and monitoring performance measures and then taking corrective action where required. A system is required to identify and respond to nonconformities, corrective actions and preventative actions. Normally, the auditor would expect to find an up-to-date action recording and tracking system.

Category 12: Incident Investigation

The organisation should have a system to record, investigate and learn from health and safety incidents that occur. In order to achieve this, the system should

- Record the incident
- Determine the underlying health and safety deficiencies (root cause)
- Identify opportunities for preventive action and continual improvement
- Communicate the results of the investigation
- Implement the preventative actions in a timely manner

Category 13: Management Review

Senior management must undertake a review of the health and safety management system periodically to ensure its suitability and effectiveness, taking into account relevant internal and external changes and the appropriateness of current resources. The review must consider the records of

- Internal Level 1 audits
- Regulatory compliance audits
- Results of worker health and safety consultations
- Health and safety performance monitoring results
- Extent to which health and safety objectives/plan have been met
- Learning from incident investigations
- Status of outstanding corrective actions
- Follow-up actions from previous management reviews
- Changing circumstances – new assets or changes in legal requirements

At the time of writing, the replacement for OHSAS 18001, which is ISO 45001, is not formally published, albeit available in draft form. The next section deals with the comparisons between the old and new standards so far as they are known at the end of 2017.

COMPARISON BETWEEN OHSAS 18001 AND ISO 45001 (DRAFT)

The new draft standard represents a sensible evolution from OHSAS 18001 and aligns with the plan–do–check–act principles and format of the other equivalent international standards, so that

- The overall intent is retained to manage the prevention of fatalities, injury and ill health.
- The focus on the role of top management in an effective OH&S management system is maintained and enhanced
- There remains a very strong focus on hazard, risk and effective control of risk.

ISO 45001 introduces a small number of requirements that are largely new when compared with OHSAS (new clause numbers are shown in brackets), including the following:

- Understanding the organisation and its context (4.1)
  - 'The organisation shall determine external and internal issues that are relevant to its purpose and objectives and that affect its ability to achieve the intended outcome(s) of its OH&S management system.'
- Understanding the needs and expectations of workers and other interested parties (4.2)
  - 'The organisation shall determine:
    a. the workers and other interested parties that are relevant to the OH&S management system;
    b. the requirements of these interested parties and which of these are added to applicable legal and other requirements.'
- Action to address risks and opportunities (6.1)
- Assessment of risks to the OH&S management system (6.1.2.2)
  - 'The organisation shall establish, implement and maintain a process for the on-going proactive identification of hazards arising in the workplace, and to workers.'
- Identification of OH&S opportunities (6.1.2.3)
  - 'The organisation shall establish, implement and maintain a process to:
    a. assess OH&S risks from the identified hazards taking into account applicable legal and other requirements, the effectiveness of existing controls and taking into consideration the hierarchy of controls;
    b. identify opportunities to eliminate or reduce OH&S risks.'
- Planning to take action (6.1.4)
  - 'The organisation shall plan:
    a. actions to address these the risks and opportunities;
    b. actions to address applicable legal and other requirements;
    c. actions to prepare for, and respond to, emergency situations;
    d. how to integrate and implement the relevant actions, including the determination and application of controls, into its OH&S management system processes;
    e. how to evaluate the effectiveness of these actions and respond accordingly.'

Consolidated Requirements

The new standard consolidates a number of existing requirements that were previously distributed across a number of clauses of OHSAS 18001 and rationalises them into stand-alone requirements.

For example:

- Management of change, which was previously referred to in five separate clauses, is now consolidated into the new section 8.2.
- Outsourcing, procurement and contractors requirements, which were previously referred to in eight separate and rather randomly dispersed clauses, are now consolidated into the new sections 8.3, 8.4 and 8.5.
- Continual improvement, which was previously referred to in six separate clauses, is now consolidated into the new section 10.2.

There are also minor alterations to the following clauses in the new draft standard ISO 45001:

- Scope (4.3)
- Leadership and Commitment (5.1)
- OH&S Policy (5.2)
- Organisational Roles, Responsibilities, Accountabilities and Authorities (5.3)
- Hazard Identification (6.1.2.1)
- OH&S Objectives (6.2.1) and Planning to Achieve (6.2.2)
- Information and Communication (7.4)
- Operational Planning and Control (8.1.1)
- Hierarchy of Controls (8.1.2)
- Outsourcing (8.3)
- Emergency Preparedness (8.6)
- Monitoring, Measurement, Analysis and Evaluation (9.1)
- Internal Audit (9.2)
- Management Review (9.3)
- Incident, Nonconformity, Corrective Action (9.1.1)
- Continual Improvement (10.2)

From and auditing point of view, with the exception of the six new requirements mentioned at the beginning of this section, the auditor should notice very little change in what is expected of him or her.

GUIDELINES FOR AUDITING MANAGEMENT SYSTEMS ISO 19011

The international standard ISO 19011:2011 has already been referred to on various occasions throughout this book. For completeness, this brief reference is included in this chapter on relevant international standards. This standard focuses primarily

on setting up the audit programme and provides some useful advice for organisations doing that for the first time. That advice has been referred to and substantially expanded on throughout this book.

What this standard does not help with is detailed advice on how to conduct an efficient and effective audit and still be able to maintain cordial relationships between the auditors and auditee. However, new auditors and organisation's audit managers are recommended to become familiar with the contents of the auditing standard ISO 19011.