

ISO/IEC 27001:2022 INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION – INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS) AUDITOR / LEAD AUDITOR

40 HOUR VILT TRAINING COURSE

CQI / IRCA CERTIFICATED COURSE 2549 – PR 373

LEARNER GUIDE

SGS ACADEMY

SGS

CQI and IRCA Certified Training

Welcome to your CQI and IRCA Certified ISO 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems (ISMS) Auditor / Lead Auditor Course.

SGS United Kingdom Ltd has been independently assessed and approved by the CQI and IRCA. This means they have the processes and systems in place to deliver certified courses to the highest standard.

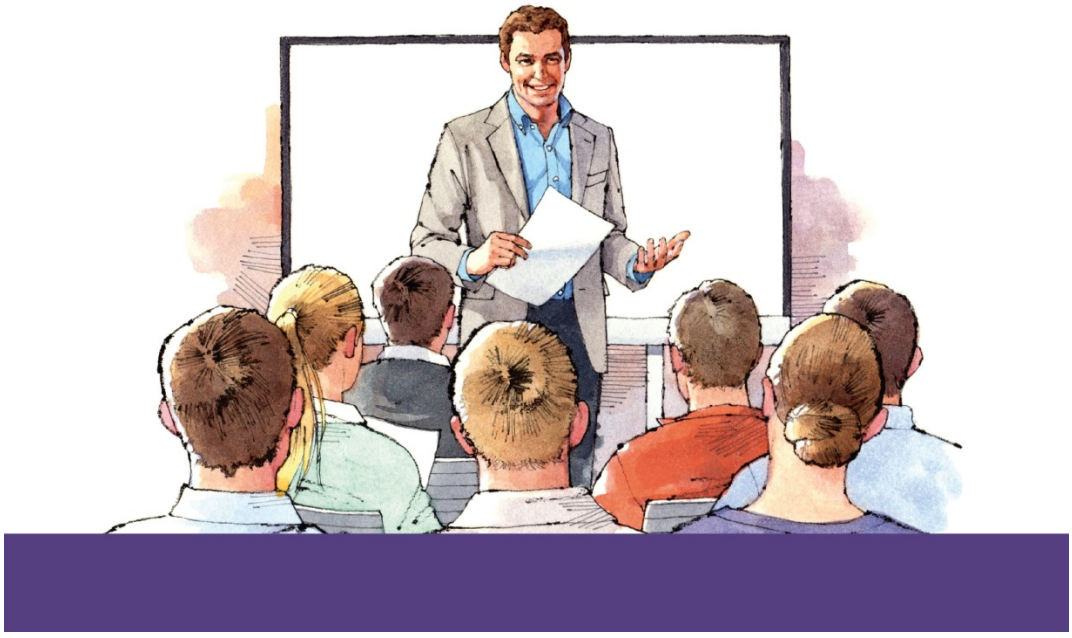
About the CQI and IRCA

The CQI is the only chartered professional body dedicated entirely to quality.

IRCA is its specialist division dedicated to management system Auditors.

Find out more about the CQI and IRCA at www.quality.org.

We hope you enjoy your course.



CONTENTS PAGE

COURSE ADMINISTRATION....4
SESSION ONE....14
ISMS AND THE ISO/IEC 27000 SERIES OF STANDARDS....14
SESSION TWO....34
PROCESS-BASED ISMS....34
SESSION THREE....69
REGISTRATION, CERTIFICATION AND AUDITOR COMPETENCE....69
SESSION FOUR....88
AUDITS: DEFININTION, PRINCIPLES AND TYPES....88
SESSION FIVE....101
THE AUDIT PROCESS....101
SESSION SIX....120
PREPARING FOR THE ON-SITE AUDIT (AUDIT STAGE 1)....120
SESSION SEVEN....137
DEVELOPING THE CHECKLIST....137
SESSION EIGHT....147
CONDUCTING THE ON-SITE AUDIT (AUDIT STAGE 2)....147
SESSION NINE....167
AUDIT REVIEW....167
SESSION TEN....187
AUDIT REPORTING AND FOLLOW-UP (STAGE 2)....187
APPENDICES....210

COURSE ADMINISTRATION

FOREWORD

This course is certificated by the Chartered Quality Institute and International Register of Certificated Auditors, Course Certification Number, 2549 – PR 373.

Learners who successfully complete this course may be eligible to apply for certification by the CQI and IRCA as an Auditor, Lead Auditor or Internal Auditor within five years of course completion.

Other requirements for certification are outlined in www.quality.org.

This material is owned by SGS United Kingdom Ltd and is provided internationally as SGS Knowledge (Kn). The SGS policy and objectives with respect to the course are given below.

POLICY STATEMENT AND OBJECTIVES

It is the policy of SGS United Kingdom Ltd to provide Auditor/Lead Auditor training courses which meet the requirements set by the Chartered Quality Institute and International Register of Certificated Auditors (CQI and IRCA).

The aim of this course is to provide learners with the knowledge and skills required to perform first, second and third-party audits of information security management systems against ISO/IEC 27001 (with ISO/IEC 27002), in accordance with ISO 19011 and ISO/IEC 17021, as applicable.

CQI / IRCA COURSE CRITERIA – OBJECTIVES

Upon completion of this course, learners will be able to:

- Explain the purpose and business benefits of an ISMS, of information security management systems standards, of management system audit and of third-party certification.
- Explain the role of an Auditor to plan, conduct, report and follow-up an ISMS audit in accordance with ISO 19011 and ISO/IEC 17021, where appropriate.
- Plan, conduct, report and follow-up an audit of an ISMS to establish conformity or otherwise with ISO/IEC 27001 (with ISO/IEC 27002) in accordance with ISO 19011 and ISO/IEC 17021 where appropriate.

Learners will need to demonstrate acceptable performance in these areas to complete the course successfully.

PRIOR KNOWLEDGE

Before starting this course, learners are expected to have the following prior knowledge:

- Management systems.
- Understand the Plan-Do-Check-Act (PDCA) cycle.
- Information security management.

PRIOR KNOWLEDGE, CONTINUED

- Knowledge of the following information security management principles and concepts:
  - Awareness of the need for information security.
  - The assignment of responsibility for information security.
  - Incorporating management commitment and the interests of stakeholders.
  - Enhancing societal values.
  - Using the results of risk assessments to determine appropriate controls to reach acceptable levels of risk.
  - Incorporating security as an essential element of information networks and systems.
  - The active prevention and detection of information security incidents.
  - Ensuring a comprehensive approach to information security management.
  - Continual reassessment of information security and making of modifications as appropriate.

ISO/IEC 27001

Knowledge of the requirements of ISO/IEC 27001 (with ISO/IEC 27002) and the commonly used information security management terms and definitions, as given in ISO/IEC 27000 (overview and vocabulary), which may be gained by completing a CQI and IRCA certified ISMS Foundation Training Course or equivalent.

COURSE BRIEF

LEARNER INTRODUCTIONS

At the start of the course, learners will be asked to introduce themselves. This introduction should include information on the individual's job function, organisation, the organisation's product or service, the organisation's certification details, the individual's knowledge and understanding of the ISO ISMS standards and their expectations upon completing the course.

PARTICIPATIVE LEARNING

This course is presented using techniques that have been designed to make training an enjoyable as well as a beneficial experience. The approach is based on scientific evidence as to how the brain works and people learn. A better understanding of the standard, and the knowledge and skills of an Auditor is guaranteed.

SUCCESS CRITERIA

Learners will be graded based on:

- A continuous assessment of their performance against the course learning objectives.
- Their marks obtained in the written examination.

To successfully complete the course, learners must obtain at least:

- A pass grade in the continuous assessment.

CONTINUOUS ASSESSMENT

Throughout the duration of the course, the performance of learners will be evaluated during the course sessions, role-plays and exercises. Learners must demonstrate acceptable performance in the learning objectives to successfully complete the course.

If a learner is either not understanding the subject or not participating adequately, he or she shall be made aware of the shortfall in performance and, if appropriate, be provided with additional coaching outside the formal course hours.

Timekeeping during the course is considered during the continuous assessment of learners. Poor timekeeping may result in failure to meet course requirements. No exception will be given to extending break times for external business activities.

CONTINUOUS ASSESSMENT

In addition, learners are required to be in attendance for the full duration of the course. Failure to do so will be reflected in the learner's continuous assessment and final grade. Learners may be graded 'Excellent', 'Good', 'Satisfactory' or 'Fail' according to the tutor's perception of their overall readiness and ability to carry out third-party audits.

Learners who fail the continuous assessment, and who intend to apply for certification as an Information Security Management Systems (ISMS) Auditor, will be required by the CQI and IRCA to retake the entire course.

LEARNING OBJECTIVES

Learning objectives describe in outline what learners will know and be able to do by the end of the course. On completion, successful learners will have the knowledge and skills to:

KNOWLEDGE

- Explain the purpose and business benefits of:
  - An ISMS.
  - ISMS standards.
  - Management system audit; and
  - Third-party certification.
- Explain the role of an Auditor to plan, conduct, report and follow-up on an ISMS audit to establish conformity (or otherwise) with ISO/IEC 27001 (with ISO/IEC 27002) in accordance with ISO 19011 and ISO/IEC 17021, where appropriate.

SKILLS

- Plan, conduct, report and follow-up an audit of an ISMS to establish conformity (or otherwise) with ISO/IEC 27001 (with ISO/IEC 27002) in accordance with ISO 19011 (and ISO 17021 where appropriate).

EXAMINATION

The examination comprises a two-hour paper. Learners are allowed access to ISO 27001:2022 (or national equivalent) during the examination.

Persons carrying out the examination in a language other than their mother tongue may be allowed an additional 20% (dependant on exam delivery method) and access to a dictionary (which must be free of any annotations).

Electronic devices such as laptops and mobile phones are not permitted in the examination room.

NEW TERMINOLOGY

- Paper-based Exam: Current hard copy exam paper completed within the classroom, facilitated by live in-person invigilator.
- SGS Interim Online Exam: Current content of paper-based hard copy exam paper facilitated remotely by a live invigilator.
- New CQI and IRCA Online Exam: New content, new questions, new structure completed online using CQI and IRCA portal. Links to practice exam questions and final exam access self-enrolment.

PAPER-BASED /SGS INTERIM ONLINE EXAMS

The paper-based / SGS interim online exam is in four sections:

- Section 1 contains questions that require a brief written answer;
- Section 2 also contains questions that require brief written answers;
- Section 3 contains questions that require detailed written answers; and
- Section 4 contains a number of situations for which a Corrective Action Request (CAR) / Non-Conformance Report (NCR) may be required.

To pass the examination, learners must achieve a total of 70% overall; in addition, a minimum of 50% must be achieved in each section.

CQI AND IRCA ONLINE EXAM

Learners will have 30 days from the last day of their course to take their CQI and IRCA online exam.

The CQI and IRCA online exam is split in to five domains:

- Domain 1 – Concepts and Principles of MSS;
- Domain 2 – Audit concepts and Auditor responsibilities;
- Domain 3 – Planning the audit;
- Domain 4 – Conducting the audit; and
- Domain 5 – Reporting and closing out the audit.

The CQI and IRCA online exam will include a mix of:

- Multiple-choice (choose one correct answer);
- Multiple response (choose several correct answers);
- Fill in the blanks (drag and drop the correct words into the sentence);
- Matching (drag and drop responses to correctly match items);
- Sequencing (drag and drop responses to form the correct order);

The last two sections of the exam will include scenario questions related to conducting, reporting on, and closing out audits. Learners will be asked to evaluate the scenario and select the correct course(s) of action.

All questions will be computer-marked. Once learners have answered a question, they will not be permitted to review or change their response.

Learners must achieve the minimum pass mark for each domain and an overall score of 40 marks (50%).

To pass the examination, learners must achieve a total of 50% overall; in addition, a minimum of 38% must be achieved in each domain.

Appendix 13: CQI Learner Privacy Notice (Online Exam).

Appendix 14: CQI and IRCA Online Exams: Guide for Learners.

EXAMINATION RESIT

Learners are allowed only one re-sit, which must take place within 12 months of sitting the original examination. Learners who fail the re-sit must retake the entire course if they wish to successfully complete the course.

Re-sits are only permitted provided the learner has passed the continuous assessment and must be conducted in accordance with the course criteria of their original course.

COURSE CERTIFICATION

Learners who pass both the examination and continuous assessment will be issued with a "Certificate of Achievement" that satisfies the formal training for an individual seeking certification as a CQI and IRCA Auditor/Lead Auditor. The "Certificate of Achievement" is valid for a period of five years from the date of the last day of the examination for certifying as an Auditor/Lead Auditor with the CQI and IRCA.

Learners who do not pass the continuous assessment and have been in attendance for the full duration of the course will be issued with a "Certificate of Attendance".

Learners who fail the written examination and pass the continuous assessment will receive a "Certificate of Attendance" and will be allowed to re-sit the examination within 12 months of the end date of the original course.

Learners will receive their certificates within eight weeks of course completion.

REMINDER

The use of mobile phones, iPads, iPhones, Tablets, pagers etc. during the course is not permitted.

CONTINUOUS IMPROVEMENT

Learners are given a Course Evaluation Form at the start of the course for completion and submission at the end of the course. This provides SGS Knowledge (Kn) with important customer feedback for the continuous improvement of the course.

APPEALS AND COMPLAINTS

Learners may appeal or make a complaint about any aspect of the course or the continuous assessment. Appeals and complaints should be addressed, in writing, to Global.irca.training@sgs.com.

CQI AND IRCA GDPR PRIVACY NOTICE

Appendix 12

CQI AND IRCA MALPRACTICE AND MALADMINISTRATION

Appendix 13

SESSION ONE

ISMS AND THE ISO/IEC 27000 SERIES OF STANDARDS

ISMS AND THE ISO/IEC 27000 SERIES OF STANDARDS

OBJECTIVES

When you have completed this session, you will be able to:

- Explain the purpose and benefits of an ISMS.
- Be aware of the development and application of ISO/IEC 27001.
- Explain the purpose, content and relationship between ISO/IEC 27001 and other management system standards.
- Explain the difference between legal compliance and conformity with international standards.
- Explain the concepts on ISMS.
- Understand continual improvement based on the Plan-Do-Check-Act (PDCA) cycle.

KEY POINTS

- History of ISO/IEC 27001.
- ISMS family of standards.
- ISO/IEC 27001 requirements.
- Aims of an ISMS.
- ISMS concepts.
- Compatibility with other management system standards.
- Auditing standards.
- Legal compliance – management system standards.
- The process approach.
- Continual improvement based on the PDCA cycle.
- The benefits of ISMS.

ISMS AND THE ISO/IEC 27000 SERIES OF STANDARDS

INTRODUCTION

Information security management systems (ISMS) are intended to provide organisations with the elements of an effective information security system in order to achieve the best practice in information security and to maintain economic goals.

The intention is that these systems may be integrated with other management requirements such as those for quality and the environment.

The system upon which this course is based is:

- ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements.
- ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection Information Security Controls

These standards have been developed in response to customer demands for a recognisable standard against which ISMS can be audited and certificated.

Appendix 1 contains a number of terms and definitions that are used in the auditing of management systems.

HISTORY OF ISO/IEC 27001

In the early 1990s, the UK Department of Trade and Industry initiated the development of a British standard to cover information security. The first standard was adopted in 1995. Other developments followed:

- 1998: Certification requirements launched.
- 1999: Second edition issued; this added e-commerce to the scope of the standard.
- 2000: ISO approved ISO 17799 Part 1.
- 2002: BS 7799-2:2002 issued on 5th September; this revision adopted the “process model” which brought the standard into line with ISO 9001 and ISO 14001.
- 2005: ISO/IEC 27001 and ISO/IEC 27002 issued.
- 2013: ISO/IEC 27001 re-issued having been revised in line with other ISO management systems standards.

HISTORY OF ISO/IEC 27001, CONTINUED

- 2022: Title change – ISO 27001:2022 - Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. This change aligns with the title of ISO/IEC 27002:2022 (Information Security, Cybersecurity and Privacy Protection – Information Security Controls).

ISMS FAMILY OF STANDARDS

The ISMS family of standards has been developed to assist organisations of all types and sizes to implement and operate an ISMS. The "family" of standards is set to:

- Define requirements for an ISMS and for those certifying such systems.
- Provide direct support, detailed guidance and / or interpretation for the overall Plan-Do-Check-Act (PDCA) processes and requirements.
- Address sector-specific guidelines for ISMS, and
- Conformity assessment for ISMS.

These include:

- **ISO/IEC 27000** - Information Security Management Systems — Overview and Vocabulary
- **ISO/IEC 27001** - Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements
- **ISO/IEC 27002** - Information Security, Cybersecurity and Privacy Protection – Information Security Controls
- **ISO/IEC 27003** - Information Security Management System Implementation Guidance
- **ISO /IEC 27004** - Information Security Management — Measurement
- **ISO/IEC 27005** - Information Security Risk Management. This international standard supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach
- **ISO/IEC 27006** - Requirements for Bodies providing Audit and Certification of Information Security Management Systems

ISMS FAMILY OF STANDARDS, CONTINUED

- **ISO/IEC 27007** - Guidelines for Information Security Management Systems Auditing
- **ISO/IEC 27008** - Guidelines for Auditors on Information Security Management Systems Controls
- **ISO/IEC 27010** - Information Security Management Guidelines for Inter-Sector and Inter- Organisational Communications
- **ISO/IEC 27011** - Information Security Management Guidelines for Telecommunications Organisations based on ISO/IEC 27002
- **ISO/IEC 27013** - Guidance on the Integrated Implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- **ISO/IEC 27014** - Governance of Information Security
- **ISO/IEC 27015** - Information Security Management Guidelines for Financial Services
- **ISO/IEC 27016** - Information Security Management – Organisational Economics
- **ISO/IEC 27017** - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- **ISO/IEC 27018** - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- **ISO/IEC 27019** - Information technology — Security techniques — Information security controls for the energy utility industry
- **ISO/IEC 27701** - Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27001 for privacy information management – Requirements and guidelines
- **ISO 27799** - Health Informatics — Information Security Management in Health using ISO/IEC 27002

ISO/IEC 27001:2022 INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION – INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS

GENERAL

First it is important to begin with and define the terms:

- Information Security
- Cybersecurity

Information security is defined as “preservation of confidentiality, integrity and availability of information” (ISO/IEC 27000:2018).

Cybersecurity is defined as “protection of an IT-system from the attack or damage to its hardware, software or information, as well as from disruption or misdirection of the services it provides” (ISO/TR 22100-4:2018).

The standard has been developed to provide requirements for establishing, implementing, maintaining and continually improving an information security management system.

For an organisation, taking on an ISMS is a strategic decision which is influenced by the organisation’s needs and objectives, security requirements, the organisational processes used and the size and structure of the organisation.

The ISMS preserve the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is applicable to any organisation regardless of type, size and nature of business.

The ISMS should assist in maintaining and improving competitive edge, cash flow, profitability, legal compliance and commercial image.

THE RELATIONSHIP BETWEEN ISO/IEC 27001 AND ISO/IEC 27002

As with ISO/IEC 27001, ISO/IEC 27002 Information Technology – Code of Practice for Information Security Management was prepared by the International Standards Organization (ISO). ISO/IEC 27001 sets out the requirements for an ISMS; ISO/IEC 27002 contains the very same controls as the Annex A of ISO/IEC, however with additional implementation guidance and additional information – e.g. explaining the concept of “Attributes”

Scope

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

a) within the context of an information security management system (ISMS) based on ISO/IEC 27001;

b) for implementing information security controls based on internationally recognized best practices;

c) for developing organization-specific information security management guidelines.

There are five attributes addressed in ISO/IEC 27002:2022:

a) Control type

Control type is an attribute to view controls from the perspective of when and how the control modifies the risk with regard to the occurrence of an information security incident. Attribute values consist of Preventive (the control that is intended to prevent the occurrence of an information security incident), Detective (the control acts when an information security incident occurs) and Corrective (the control acts after an information security incident occurs).

b) Information security properties

Information security properties is an attribute to view controls from the perspective of which characteristic of information the control will contribute to preserving. Attribute values consist of Confidentiality, Integrity and Availability.

c) Cybersecurity concepts

Cybersecurity concepts is an attribute to view controls from the perspective of the association of controls to cybersecurity concepts defined in the cybersecurity framework described in ISO/IEC TS 27110. Attribute values consist of Identify, Protect, Detect, Respond and Recover.

Scope, continued

d) Operational capabilities

Operational capabilities is an attribute to view controls from the practitioner's perspective of information security capabilities. Attribute values consist of Governance, Asset management, Information protection, Human resource security, Physical security, System and network_ security, Application security, Secure configuration, Identity and access management, Threat and vulnerability management, Continuity, Supplier_relationships_security, Legal and_ compliance, Information security event management and Information security assurance.

e) Security domains

Security domains is an attribute to view controls from the perspective of four information security domains: "Governance and Ecosystem" includes "Information System Security Governance & Risk Management" and "Ecosystem cybersecurity management" (including internal and external stakeholders); "Protection" includes "IT Security Architecture", "IT Security Administration", "Identity and access management", "IT Security Maintenance" and "Physical and environmental security"; "Defence" includes "Detection" and "Computer Security Incident Management"; "Resilience" includes "Continuity of operations" and "Crisis management". Attribute values consist of Governance and Ecosystem, Protection, Defence and Resilience.

The attributes given in this document are selected because they are considered generic enough to be used by different types of organizations. Organizations can choose to disregard one or more of the attributes given in this document. They can also create attributes of their own (with the corresponding attribute values) to create their own organizational views. Clause A.2 includes examples of such attributes

Not all the controls in ISO/IEC 27001 Annex A may be applicable and indeed other controls may be required depending on the size and complexity of the organisations and its products and the competency levels of its personnel.

ISO/IEC 27002 makes the point that the recommendations should be selected and used in accordance with applicable laws and regulations.

AIMS OF ISMS

The development of an ISMS represents a “proactive", systematic and logical approach to address the problems of information security, rather than the “reactive”, piecemeal approach to security breaches.

Organisations are subject to increasing information security risks. These may be internal (within the organisation) or external (the result of factors outside of the organisation).

The organisation may respond through:

- corporate vision and policies;
- corporate cultures, values;
- marketing and communication; and
- establishing an ISMS.

ISO/IEC 27001 is an attempt to unify and set a framework to the approach to ISMS.

ISMS CONCEPTS

The concepts that underpin information security are:

- Confidentiality - Ensuring that information is accessible only to those authorised to have access.
- Integrity - Safeguarding the accuracy and completeness of information and processing methods.
- Availability - Ensuring that authorised users have access to information and associated assets when required.

The ISMS is best viewed as an organising framework that needs to be continually monitored and periodically reviewed to provide effective direction for an organisation’s information security activities in response to changing internal and external factors.

Every individual in an organisation should accept responsibility for information security improvements.

COMPATIBILITY WITH OTHER ISO STANDARDS

One of the strengths of ISO/IEC 27001 is that the structure of the standard very closely follows that of existing international management system standards.

COMPATIBILITY WITH OTHER ISO STANDARDS, CONTINUED

It has the same structure; identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives and thereby are compatible with other management system standards that have adopted Annex SL.

It is intended that this common approach will enable organisations to integrate two or more other management system standards to a single management system meeting all requirements.

- The ISO 9000 series of Quality Management System Standards - Set out the fundamental, requirements and guidelines for the implementation, operation and performance improvement for effective quality management systems.

  Many of the definitions found in ISO/IEC 27000 are taken from ISO 9001 Quality Management Systems – Fundamentals and Vocabulary.

- ISO 14001 Environmental Management Systems – Specification with Guidance for Use – Set out the requirements for environmental management systems and contains guidance for the implementation of the requirements.

- ISO 45001 Occupational Health and Safety Management Systems – Requirements – Set out the specifications for an occupational health and safety management system standard against which management systems may be audited and certificated.

- ISO 22301 Societal Security – Business Continuity Management Systems – Requirements – Set the requirements for a documented management system to protect against and revoke from disruptive incidents when they occur.

AUDITING STANDARDS

- ISO 19011 Guidelines for Auditing Management Systems Auditing - Whilst ISO 19011 is only a guidance document, it does provide detailed information on the planning and implementation of effective auditing. This is vitally important to organisations carrying out audits of suppliers and to certification bodies.

- ISO/IEC 17021 Conformity Assessment – Requirements for Bodies providing Audit and Certification of Management Systems - This is a requirements standard intended for use by accreditation bodies (for example: UKAS, ANAB, DAkkS RvA) to assess management systems certification bodies (SGS, BSI, BVQI, LRQA etc.).

LEGAL COMPLIANCE – MANAGEMENT SYSTEMS STANDARDS

The progressive development of customer-driven standards and the increase in world-wide legislation especially involving environmental, health and safety obligations is focusing organisations on developing integrated management systems to address legal requirements and process-based management systems.

Implementation of these systems alone will not bestow immunity from organisational liability or prosecution, but will significantly reduce the risks if the systems are maintained effectively.

Auditors conducting audits on information security management systems and integrated management systems will have to be aware of the management systems standards and the legal requirements of the respective countries where they are conducting the audits.

In this respect, there is significant difference between legal compliance and conformance with management systems standards.

Where an organisation is not in compliance with legal requirements, the organisation may be liable to prosecution.

If an organisation's ISMS are not in conformance with ISO/IEC 27001, third-party certification may be withdrawn but the organisation will not be liable to prosecution.

Auditors conducting ISMS audits identify, by evidence, areas of conformity and nonconformity to ISO/IEC 27001 through their formal reporting system.

Where there is evidence of nonconformity to legal requirements, it is advisable to bring this to the attention of the organisation management who then have the responsibility to take appropriate action through their quality, environmental and/or their health and safety control systems.

Where Auditors are appropriately trained and conducting integrated management system audits, they are required to report both legal compliance and ISO conformance against the audit evidence.

THE BENEFITS OF ISMS

The establishment and operation of an ISMS will not, in itself, necessarily result in immediate reduction in adverse information security risks. Essentially, an ISMS is a tool that enables an organisation to achieve and systematically control the level of information security performance that it has set.

THE BENEFITS OF ISMS, CONTINUED

The system should provide economic benefits such as:

- reduced security breach investigation time;
- reduced process training and new staff;
- reduced litigation;
- reduced legal fees;
- possible reductions in insurance premiums;
- increase in commercial / public image;
- protection of information assets;
- increase in information security awareness;
- improvement in staff recruitment;
- increased confidence with customers and other interested parties.

When certified to ISO/IEC 27001 by an independent certification body such as SGS, BVQI or Lloyds Register, the organisation benefits by:

- lower risk of data breaches;
- improved profile and credibility;
- competitive advantage in the market place;
- reduced threat from the “security image” of competitors;
- valuable input from third-party Auditors;
- employee pride and motivation;
- reduced risk of non-tariff barriers;
- meeting present or future anticipated demands of customers;
- potentially lower levels of regulatory reporting.

ACTIVITY ONE: ISMS AWARENESS

PURPOSE

- To review your understanding of ISMS. The questions are based on the prior knowledge requirements for learners set by the CQI and IRCA.

TASK

- In your team:
  - Answer the questions in the boxes provided on the following page.

OUTPUT

- Prepare to feedback your responses for discussion with the whole group.

TIME ALLOWED

- Activity: 30 minutes.
- Feedback: 15 minutes.

QUESTIONS

1) What are the key benefits for an organisation to implement an ISMS?

2) Explain the difference between the terms ‘risk analysis’ and ‘risk evaluation’.

3) What is the meaning of the term ‘risk assessment’?

4) What are the options for treating information security risks?

5) What will a methodical assessment of the risks to the organisation's information assets involve?

6) The determination of appropriate controls to reach acceptable levels of risk must take account of what?

7) How should an organisation ensure authorised user and prevent unauthorised access to systems and services?

8) What restrictions should be placed on the installation of software in an organisation?

9) What is the Plan-Do-Check-Act cycle for continual improvement?

10) If you discover that the organisation is in breach of legislation, what actions must you take?

SESSION TWO

PROCESS-BASED ISMS

PROCESS-BASED ISMS

OBJECTIVES

When you have completed this session, you will be able to:

- Understand the steps needed to establish an information security system.
- Explain the PDCA framework and its significance to ISO/IEC 27001 and information security management processes.
- Outline the processes involved in establishing, implementing, operating, monitoring, reviewing, maintaining an ISMS including the significance for ISMS Auditors.
- Understand the formulation of information security policy and objectives.
- State the requirements for ISMS documentation.
- Understand the role of the Auditor in assessing the organisation's operation control measures, risk assessment, risk treatment and Statement of Applicability (SoA).
- Explain the difference between documented information, procedures and records.
- Understand the purpose of controlling documented information.
- Understand how audits can be used as a tool for the maintenance and improvement of management systems.
- Explain the role of the ISMS Auditor in assessing the effectiveness of an organisation's ISMS.

KEY POINTS

- Application of PDCA cycle.
- Context of the organisation.
- Leadership.
- Information security policy and objectives.
- Planning.
- Support.
- Documented information.
- Control of documented information.

KEY POINTS, CONTINUED

- Competence and awareness.
- Operation.
- Performance evaluation.
- Continual improvement.
- Nonconformity and corrective action.

PROCESS-BASED ISMS

INTRODUCTION

Session One considered the reasons that organisations set up an ISMS and adopt the information security concepts that should guide such systems.

This session addresses the elements that comprise the establishment and management of an ISMS based upon the process approach set out in the ISO standards including ISO/IEC 27001:2022 and described in the ISO publication, Proposals for Management Systems, Annex SL and considers the implications for Auditors.

PROCESS APPROACH

For an organisation to function effectively, management has to identify and co-ordinate numerous linked activities. An activity that takes “inputs” and converts them to “outputs” can be considered as a “process”.

Very often the output from one process becomes the input for another process.

Therefore, organisations may comprise a number of linked processes that need to be identified and managed.

The process approach, therefore, is the systematic identification and management of these activities and the interactions between activities.

Used properly, the process approach provides control over the processes, the links between processes, and the combination and interaction of processes.

The process-approach emphasises the importance of:

- the understanding and fulfilment of requirements;
- the need to consider processes in terms of added value;
- obtaining results of process performance and effectiveness; and
- the continual improvement of processes based on objective measures.

CONTINUAL IMPROVEMENT BASED ON THE PDCA CYCLE

The process approach is based upon the methodology known as Plan-Do-Check-Act (PDCA).

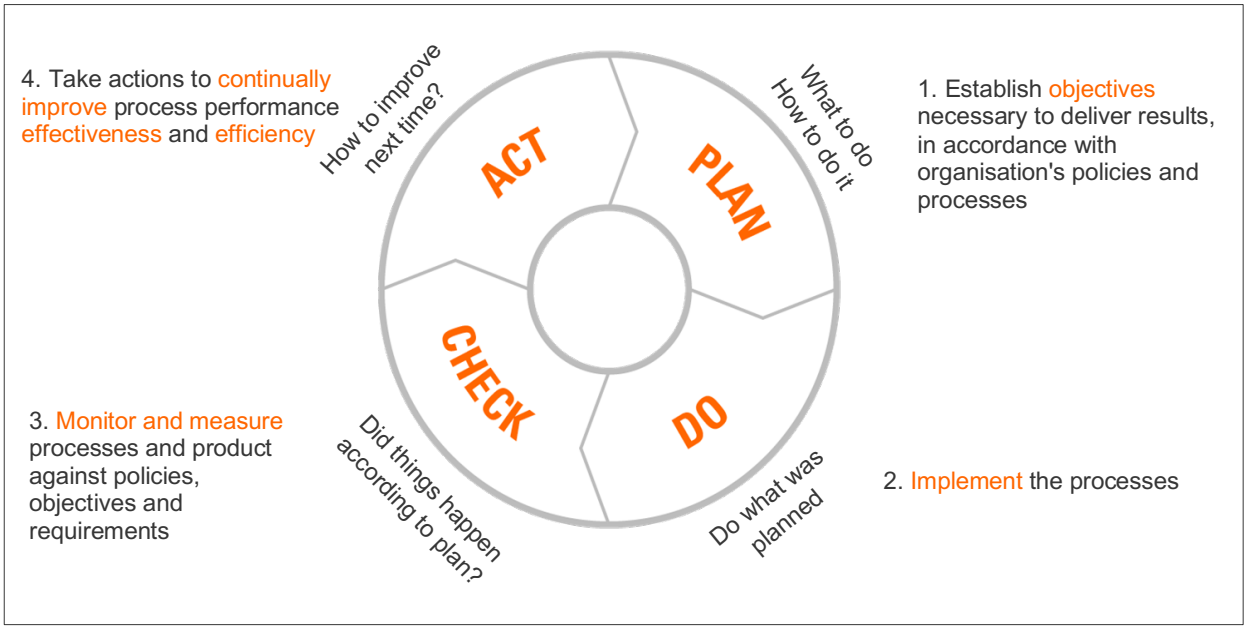
- Plan
  - Establish information security policy, objectives, targets, controls, processes and procedures relevant to improving information security in order to deliver results that align with the organisations overall policies and procedures.
- Do
  - Implement and operate the information security policy, strategies and procedures.
- Check
  - Monitor and review performance against information security policy, strategies, report results to management for review, and determine and authorise actions for remediation and improvement.
- Act
  - Maintain and improve the ISMS by taking corrective actions based on the results of the management review and re-appraising the scope of the ISMS and information security policy and objectives.

This approach to information security management that incorporates the PDCA cycle within each activity is set out in the “PDCA Cycle Applied to ISMS Diagram” below.

Information security management, thereby, becomes no longer a separate '“policing” function but is an integral part of business management because it has the ability to affect the ‘bottom line’.

This methodology is set within the clauses and requirements of Annex SL and therefore ISO/IEC 27001:2022. A diagram showing the PDCA cycle and continual improvement is shown overleaf.

PLAN-DO-CHECK-ACT CYCLE AND CONTINUAL IMPROVEMENT

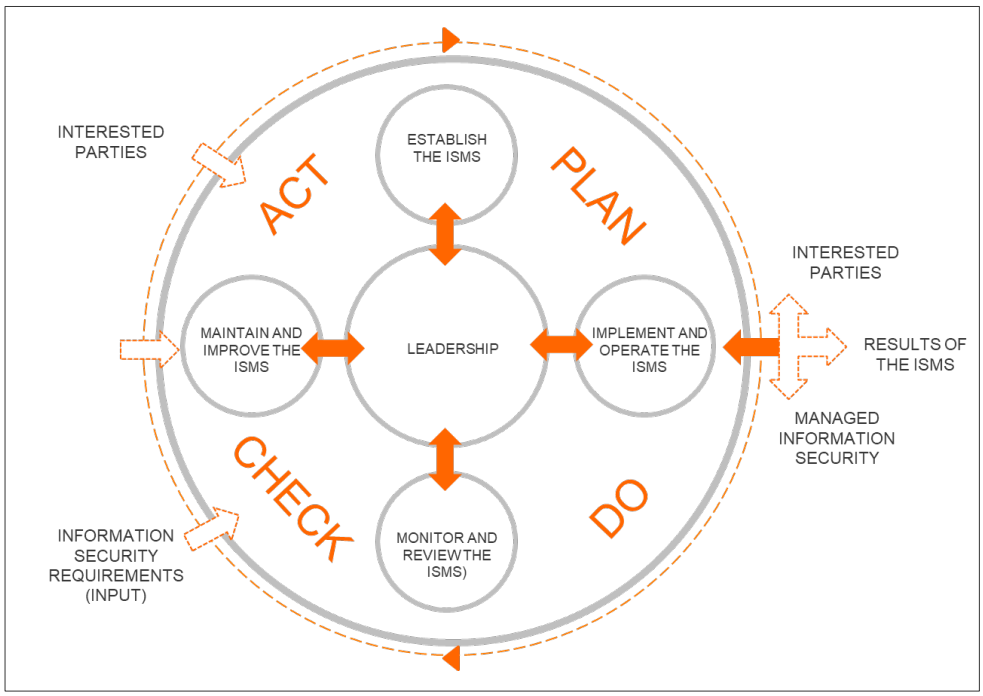


APPLICATION OF THE PDCA CYCLE

COMPONENTS OF PDCA IN ISO/IEC 27001

The Plan-Do-Check-Act model described above and shown in the diagram below.

Continual improvement of the ISMS



COMPONENTS OF PDCA IN ISO/IEC 27001, CONTINUED

The diagram 'PCDA cycle applied to an ISMS' sets out the structure and elements of a process as addressed by Clauses 4 to 10 of ISO/IEC 27001 and is addressed in ISO/IEC 27001 as follows:

- Clause 5 is a component of "Plan". It summarises the requirements specific to top management's role in the ISMS, and how leadership communicates its expectations to the organisation through a policy statement.
- Clause 6 is a component of "Plan". This clause supports ISMS through determination of actions needed to address issues raised in the assessment of risk to information security, the application of a risk treatment process and the establishment of objectives and appropriate plans to meet these objectives.
- Clause 7 is a component of "Plan". This clause supports ISMS operations as they relate to establishing competence and communicating on a recurring / as-needed basis with interested parties, while documenting, controlling, maintaining and required documentation to manage information security.
- Clause 8 is a component of "Do". It defines ISMS requirements to plan, control, and identify risk assessment and the treatment of risks.
- Clause 9 is a component of "Act". The clauses summarise the requirements necessary to measure information security management, compliance with ISO/IEC 27001, management's expectations, and seeks feedback from management regarding expectations.
- Clause 10 is a component of "Act". It identifies and acts on ISMS non-conformance through corrective action.

PLAN

Scope of ISO/IEC 27001 (Clause 1)

Clause 1 of ISO/IEC 27001 simply explains that the Standard sets out the requirements for establishing, implementing, maintaining and continually improving an ISMS within the context of the organisation.

The 'scope of an individual organisation's ISMS' is an entirely separate issue – see 4.2.5 below.

Scope of ISO/IEC 27001 (Clause 1), continued

Evidence of the effectiveness of information security may be obtained from the general level of compliance with ISO/IEC 27001 in terms of the number and significance of non-conformances found.

Evidence of reasonable expectations could be based on industry best practices, the level of access to industry information, the competence of staff and / or the technological resources of the organisation.

Application of the Standard (Clause 1)

The requirements are generic and applicable to all organisations, regardless of type, size and product or service provided.

There can be no exclusion to any of the requirements set out in Clauses 4 to 10. Exceptionally, there may be exclusions to specific Annex A requirements, which must be justified in the scope – see below.

However, the organisation is required to produce a Statement of Applicability (SoA) which contains the necessary controls needed to ensure information security.

The statement must include justification for inclusions whether they are included or not and the justification for any exclusions of control from Annex A controls. Below are some examples of ISMS scopes:

- The provision and protection of hosted learning management platforms, content and tools, customer and company data and associated infrastructure. The management and monitoring of hosted service providers, in accordance with the Statement of Applicability version 1.2.
- The provision of an Information Security Management System that supports Construction, Civil Engineering, Facilities Management, Frameworks, and Specialist Joinery in accordance with Statement of Applicability version 1.10.
- The provision of network rental and hosting services, for both firewall and server equipment, at ABC's data centre in Taipei City, in accordance with the Statement of Applicability, version 1.01.

Understanding the organisation and its context

Clause 4 focuses on the planning aspects of the ISMS. It requires an organisation to establish the context of its ISMS and any associated internal and external issues (including legislation and other requirements – see legal and regulatory requirements below) as well determine its needs and those of interested parties (those who can be affected by the organisations activities), requirements and scope.

The organisation will need to determine internal and external issues that are relevant to its purpose and that effects its ability to achieve the intended outcomes(s) of its ISMS and to ensure that the ISMS is aligned to the objectives, legal and statutory obligations of the organisation.

The Auditor should "test" that the organisation has gained a thorough "understanding" of these commitments, the organisation has:

- Identified the activities, assets and resources that support the delivery of these products and services including organisation's activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact related to a breach in information security might have.
- Established links between the information security policy and the organisation's objectives and other policies, including its risk treatment plan.
- Identified interested parties and their expectations.
- Assessed the impact and consequences over time of the failure of these though the establishment of a risk treatment plan and Statement of Applicability.
- Identified and evaluated the perceived threats to the organisation and its information security.

Legal and regulatory requirements

The organisation should have:

- Identified applicable legal and regulatory obligations, statutory duties and the environment in which the organisation operates; this must also include the legal and regulatory requirements of relevant interested parties.
- Established, implemented and maintained the ISMS keeping in view all the obligations to which it subscribes.

Legal and regulatory requirements, continued

The Auditor will look for evidence that this process has actually taken place and is incorporated into the regular updating process of the ISMS.

Scope of the ISMS

Critical to the conduct of the audit is the determination of the scope of the ISMS and, thereby, the scope of the audit. The organisation must define the scope of the ISMS (Clause 4.3) and set the information security objectives taking into account the requirements of the interested parties.

These may include legal and regulatory requirements and any contractual requirements. They may also include interfaces and dependences between activities performed by the organisation and those that are performed by other organisations.

The scope should be consistent with the risk assessment and risk treatment plan undertaken by the organisation and appropriate to the size, nature and complexity of the organisation.

An Auditor will expect that the scope has taken into consideration:

- The parts of the organisation to be included.
- Products and services and relevant activities within the scope of the ISMS.
- The interested parties' needs and expectations within the ISMS scope statement.

Scope of the ISMS

The Auditor will need to establish that the ISMS scope statement is fit for the:

- Business situation of the audit client.
- Overall ISMS in terms of:
  - geographic aspects;
  - technical aspects;
  - process aspects.

Leadership

Top management and other managers must show leadership with respect to the ISMS (Clause 5.1). The standard sets out several ways by which management are able to demonstrate their commitment. One of these is through the establishment of an information security policy.

ISMS policy

The ISMS policy demonstrates the commitment of management. The policy should be appropriate to the purpose of the organisation (Clause 5.2).

The policy must provide the framework for setting information security objectives.

The Auditor will need to evaluate if the organisation has given consideration in developing the policy to:

- establish an overall sense of direction and principles for action with regard to information security;
- take into account business, legal, regulatory requirements and contractual information security obligations;
- establish criteria against which risk will be assessed and the plan for risk treatment has been defined;
- be approved by top management.

The policy defines management commitment to key ISMS issues and in so doing, not only provides direction for the system, but also provides the “ultimate accountability”.

The Auditor must therefore, ensure and seek evidence to confirm that the policy has been established by the organisation’s management. Management can be interpreted in a number of ways, however, the minimum level at which the policy should be written would be a manager(s) with the authority to allocate appropriate financial and human resources to ISMS control and improvement.

It is usual, though not mandatory, for an organisation to objectively demonstrate management commitment to the policy via the approval signature of the most senior manager responsible for the scope of activities embraced by the policy.

The policy should set out the overall sense of direction and the principles for action. It should establish the means by which objectives are set, the responsibilities and performance required for the ISMS. The policy should demonstrate the formal commitment of management towards information security.

ISMS policy

The policy is probably the most important step in implementing an effective ISMS. The policy is a documented, publicly available statement indicating the organisation's commitment and intents regarding information security issues.

The policy statement must be available as documented information and communicated within the organisation.

The Auditor must ensure that employees at all levels of the organisation are aware of the information security policy and that the issues contained within it are understood, implemented and maintained.

The means by which the policy is made publicly available must be identified by the organisation and can vary from site to site. The policy may be available only upon request, be published in a report, or displayed in a public place.

There will also be a need to check that the policy is communicated to everyone working for, or on behalf of, the organisation, such as sub-contractors, temporary staff and remote workers and that they are aware of its implications for their own role and responsibilities.

Framework for continual improvement

The policy should provide the framework for continual improvement of the ISMS. Typically, the policy would indicate those specific or critical areas where continual improvement is being sought.

An Auditor would expect an organisation to demonstrate that management system improvements had the potential to improve ISMS performance; that is, "cosmetic" system improvements alone would not be acceptable.

The general approach to continual improvement through the ISMS should be set by the policy and be reflected by the individual elements of the objectives and targets.

The focus for the continual improvement as written into policy will depend largely upon the nature of the organisation's activities. Supporting information should be available in the form of documented objectives / targets and the process documentation.

Framework for continual improvement, continued

During the review or audit of the ISMS, the policy will need to be referred to frequently, in order to ensure that the objectives and targets as well as the review itself are consistent with the policy statements. It is therefore important that the wording of the policy is unambiguous and does not contain lofty, esoteric statements that are difficult to demonstrate, measure and achieve.

Roles and responsibilities

Top management must ensure that responsibilities and authorities for relevant roles must be assigned within the organisation by top management and communicated (Clause 5.3).

In particular for ensuring that the ISMS meet the requirements of the Standard and for reporting on the performance of the ISMS to top management.

One way of doing this is through organisation charts and scopes of responsibility, and these may well be presented in an ISMS Manual, although a manual in itself is not a requirement.

If the ISMS is going to operate successfully then everyone within the organisation must be aware of their particular responsibilities with regard to the processes within the organisation.

The organisational chart should therefore be drawn up to include information security as well as the other business responsibilities. All levels of management and workforce should be included since, like health and safety issues, staff at all levels can generate nonconformity if they do not operate according to the set processes.

Together with such defined authority and associated responsibilities must come the ability to act when required to do so. This will also be defined within the ISMS both in terms of the organisation and the resources available.

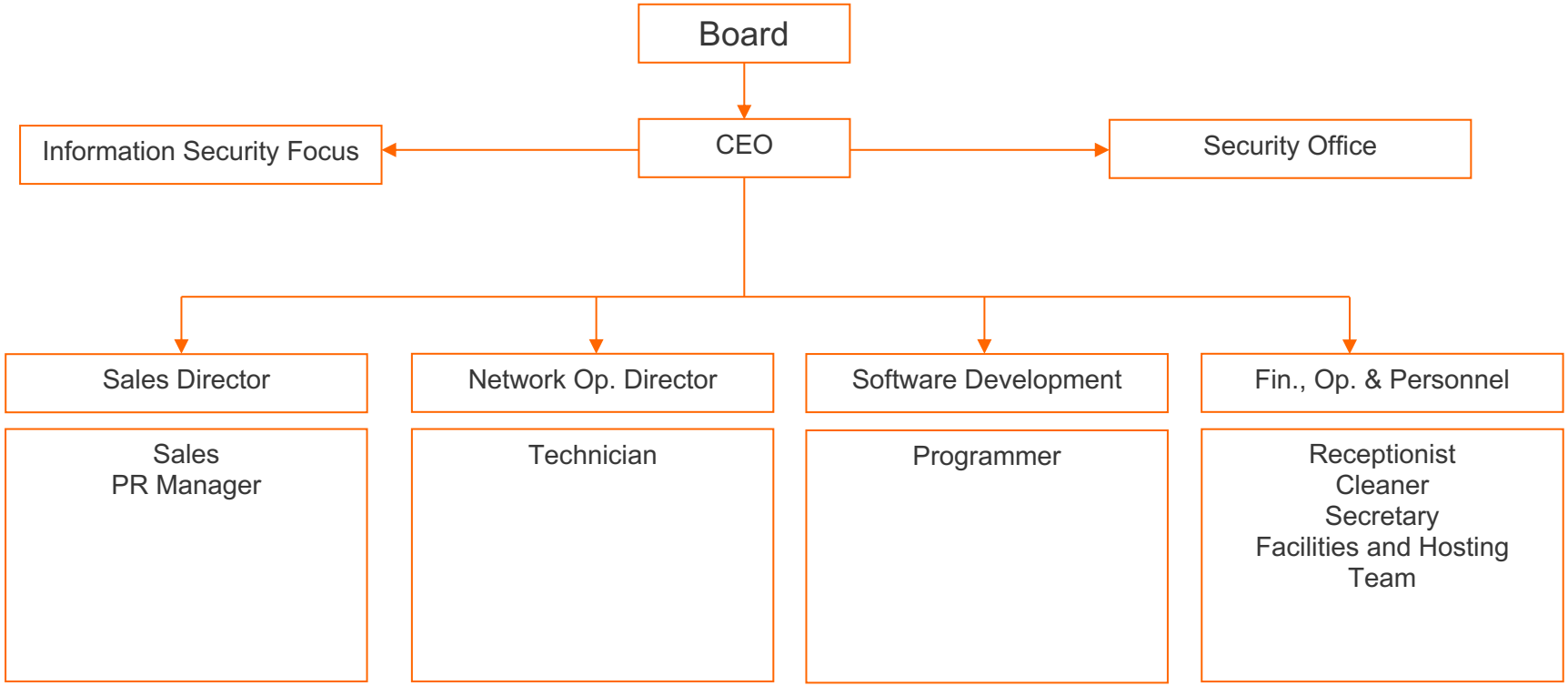
However, quite often, job descriptions, procedures and organisation charts do not tally (i.e. a certain role in the job description does not correspond to what is written in a certain procedure, or does not appear in the organisation chart).

This happens because organisation charts, job descriptions and ISMS documents are updated by different functions at different times. An Auditor should be aware of this problem, because it generates confusion within the organisation.

As an overall comment, it is always difficult to keep different lists of similar information up to date and coherent.

On the following page is an example of an organisation structure.

ORGANISATION STRUCTURE



Risk assessment and risk treatment

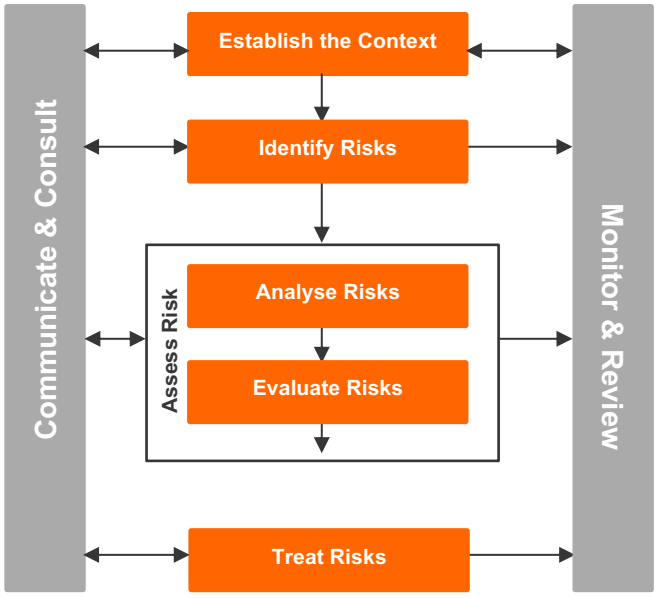
Consideration must be given to the risks and opportunities that need to be addressed (Clause 6.1). This will require that an ISMS risk assessment is undertaken with appropriate risk criteria having been established and appropriate risk treatments established (Clause 6.1.2).

Following the risk assessment, the organisation will need to select the appropriate risk treatment options and determine the controls needed to implement these options (Clause 6.1.3).

This is at the centre of the standard linking the clauses (4-10) to the Annex A controls. A number of possible controls are listed in Annex A of ISO/IEC 27001 but these are not exhaustive and additional objectives and controls may be necessary.

These will be set in a Statement of Applicability that will contain the necessary controls adopted by the organisation to treat its information security risks. The statement will contain the justification for any control that has been included and justification for any control that has been excluded from Annex A controls.

A risk management process is shown below.



The Risk Management Process (Source: AS / NZS 4360.)

Risk assessment and risk treatment, continued

ISO 31000 Risk Management Principles, ISO/IEC 27005, National Institute of Standards and Technology (NIST) and Information technology — Security techniques — Information security risk management, have been issued to provide guidance for organisations on the application of risk management to information security.

ISO/IEC 27001 refers organisations to ISO 31000, Risk management Principles for guidance on risk management in ISMS systems. The Auditor may encounter IS risk management processes based on this guidance and should therefore, familiarise him or herself with this standard.

Information security objectives (Clause 6.2)

The commitment in the information security policy to continual improvement is achieved through the setting and meeting of information security objectives.

The objectives should be:

- measurable and consistent with the information security policy.

The objectives will need to take into account the applicable information security requirements and result from risk assessment and risk treatments.

One option could be setting objectives as SMART:

- **S**et
- **M**easurable
- **A**chievable
- **R**ealistic
- **T**imed

Once decided, the objectives need to be communicated to the appropriate people in a way that they are able to translate these objectives into their individual contributions and should be available as documented information. An Auditor should be able to trace the “objective cascade” through the organisation.

Objectives should be monitored and reviewed periodically and revised as necessary in order to provide the means for the continual improvement of the ISMS.

The Auditor should seek, and evaluate justification of, the selection of any / all objectives and plans.

ISMS planning (Clause 6)

The Auditor must obtain evidence that appropriate plans have been established in order that the objectives will be achieved. This evidence could take the form of records of the initial setting up of the activities as well as records of the implementation, monitoring and review. Notice that the planning of objectives is included in the Clause 6.2, the same clause that sets the requirements for objectives.

There is a new sub-clause relating to planning of changes to the ISMS which states; *when the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner* (Clause 6.3).

Resources

The resources needed for the ISMS must be determined and provided.

These will include resources to identify establish, implement and maintain the ISMS, taking account of the need for the ISMS to address legal and regulatory requirements, and contractual obligations and commitments to interested parties.

Auditors should trace backwards from problems in the system to determine whether there is any link with lack of resources, both human and material. For example, information security breakdowns often result from the provision of adequate resources.

Resources need to be provided to identify and address legal and regulatory requirements, and contractual obligations; maintain adequate information security through the correct application of all controls.

Resources must be provided to carry out reviews of the ISMS, to react appropriately to the result of these reviews and to continually improve the effectiveness of the ISMS.

Support (Clause 7) – Resources, competence and awareness

Resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system must be determined and provided by the organisation (Clause 7.1).

Competency needs must be identified, reviewed and managed so that personnel can perform their roles effectively (Clause 7.2).

Support (Clause 7) – Resources, competence and awareness, continued

Employees must be aware of the relevance and importance of their activities, and how they contribute to the achievement of the information security objectives.

To operate effectively, individuals must have an understanding of the importance of information security and their contribution to maintaining information security and an understanding of the implications of information security breaches (Clause 7.3). Involving employees in the activities of the ISMS, through education, training and experience, should generate an improved degree of understanding and, therefore, commitment.

Training programmes should, therefore:

- raise awareness and establish support within the organisation for the ISMS and specific information security issues;
- help to identify the existing talent, resources and skills which can be harnessed to help the implementation of objectives and the ISMS; and
- help in the planning and preparation of accurate communications, targeted at the right level and audience.

Before being able to evaluate the adequacy and effectiveness of competence and awareness within an organisation, an Auditor must have a good understanding of the following issues:

- the ISMS policy;
- objectives and plans;
- the controls operated by the organisation;
- organisational structure and responsibility of key positions within the organisation.

The Auditor should verify whether employees are competent (as appropriate to their positions) with respect to:

- ISMS policy and objectives being known and understood;
- relevant significant information security issues and how individuals' actions affect the organisation's performance;
- defined individual responsibilities being understood, performed and an ability to relate these to the policy and objectives; i.e. what is expected of them and others, particularly how they should meet targets and/or performance indicators;
- the skills and knowledge necessary to ensure production targets and service levels are met.

Awareness (Clause 7.3)

This clause aims to ensure that information security is embedded into routine operations and management processes. This is regardless of the size of the organisation or the sector in which it operates.

The Auditor will need to ensure that those persons under the control of the organisation must be aware of the implications of not conforming to the ISMS as well as their own role during a breakdown in information security.

Communication (Clause 7.4)

This clause requires the organisation to determine what and how communication about the ISMS will be managed to both internal and external parties.

This should cover internal and external communications to various parties including the media, managing the receipt and provision of communications from interested parties.

ISMS documentation

Documented information

In numerous clauses, ISO/IEC 27001 calls for "*documented information*", one would expect to find information set out formally:

- The scope of the ISMS (4.3)
- An ISMS policy (5.2)
- The risk assessment process (6.1.2)
- The risk treatment process (6.1.3)
- Statement of Applicability (6.1.3)
- Information security objectives (6.2)
- Evidence of competence (7.2)
- Evidence that processes have been carried out as planned (8.1)
- Results of risk assessments (8.2)
- Results of risk treatments (8.3)
- Evidence of the results on monitoring and measurement activities (9.1)

ISMS documented information, continued

- Internal audit programmes and audit results (9.2)
- Result of management reviews (9.3)
- Nonconformities and outcome of corrective actions (10.2)

Besides these, explicitly required documented information by ISO/IEC 27001 the standard also requires:

- The organisation to maintain documented information determined by the organisation as being necessary for the effectiveness of the information security management system.

One of the most frequently overlooked section of Clause 7.5.3 Control of documented information is: *Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled*.

One of the tasks for the Auditor is to be aware that the documentation is structured to fit:

- The size of the organisation and type of activities.
- The scope of the ISMS.
- Complexity of information security requirements and the system being managed.

Documented Information is virtually anything that provides information. It may be a record, procedure, specification, drawing or report.

The information may be presented on paper, magnetic tape, computer disc, photograph, master samples or a combination of these. The flexible approach of the Standard is intended to enhance the implementation, maintenance and improvement of the system. This being the case, management should decide upon structure and format of the documentation that is needed to support the ISMS. The nature and extent of the documentation should depend upon, and meet, the needs of the organisation.

Procedures

A procedure sets out a specified way to carry out an activity or process.

Procedures are implemented, therefore, as “stand-alone” entities, designed to complete a task and in general to satisfy particular rules or requirements.

Procedures, continued

They tend to be static, defining a sequence of events necessary to complete a task.

Procedures are now required in Annex A:

- 5.4 Management responsibilities
- 5.10 Acceptable use of information and other associated assets
- 5.13 Labelling of information
- 5.14 Information transfer
- 5.19 Information security in supplier relationships
- 5.21 Managing information security in the information and communication technology (ICT) supply chain
- 5.26 Response to information security incidents
- 5.28 Collection of evidence
- 5.32 Intellectual property rights
- 5.37 Documented operating procedures
- 8.5 Secure authentication
- 8.19 Installation of software on operational systems
- 8.32 Change management

But, the standard does not always require a documented procedure. Documented procedures are only required in:

- 5.26 Response to information security incidents
- 5.37 Documented operating procedures

Procedures can be hard-coded into a (computer-) system.

Other documents

There may be other documents required by the organisation to ensure the effective planning, operation and control of its processes. Such documents may include:

Other documents, continued

- Acceptable use of information and other associated assets (Annex A.5.10)
- An inventory of information and other associated assets, including owners, shall be developed and maintained (Annex A.5.9)
- Documented operating procedures (Annex A.5.37)
- Confidentiality or non-disclosure agreements (Annex A.6.6)
- Principles for engineering secure systems to system development activities (Annex A.8.27)
- Procedures for managing information security incidents by defining, establishing, and communicating information security incident management processes, roles and responsibilities (A.5.24)
- Procedures for the identification, collection, acquisition and preservation of evidence related to information security events (Annex A.5.28)
- Legal statutory, regulatory and contractual requirements (A.5.31)
- Configuration management (A.8.9)
- Process flowcharts
- Organisation charts
- Production schedules
- Work instructions
- Operating instructions
- Job cards
- User manuals
- Inspection plans
- Test methods and instructions
- Drawings
- Approved supplier lists
- Technical manuals
- Manufacturer's recommendations
- Performance standards

Documented information as evidence (records)

The organisation needs to maintain records to provide evidence of conformity to requirements and for determining the effectiveness of the ISMS.

Annex A – 5.33 – Protection of records

Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised absence.

From the point of view of a third-party Auditor, records are one of the system attributes that ensure that it is auditable. From the point of view of the ISMS, the same applies, together with the need to provide management information.

In some cases, an Auditor will be required to use skill, judgement and practical experience to evaluate whether minimal record-keeping conforms with the requirements of the standard, and whether those minimal records, together with evidence gathered by interview, and witnessed practices, establish conformity of other elements within the system.

In order to demonstrate compliance with the standard's requirements there are many other needs for record keeping; for example, documented information in:

- 4.3 Scope of the ISMS
- 5.2 Security policy
- 6.1.2 Risk assessment process
- 6.1.3 Risk treatment process
- 6.2 Information security objectives
- 7.2 Competence
- 7.5.1 Documented information determined by the organization as being necessary for the effectiveness of the information security management system
- 8.1 Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned
- 8.2 Result of risk assessment
- 8.3 Result of risk treatment
- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2.2 Audit program and audit results

Annex A – 5.33 – Protection of records, continued

- 9.3.3 Results of management review
- 10.2 Nonconformity and corrective action

Records should be simple, legible readily identifiable and retrievable. They should provide management with useful information for continual improvement and data for improving ISMS processes.

Records may appear in any form which means that in many organisations, records will be held electronically.

Control of documented information

All documented information has to be controlled.

In some organisations the issuing and approval authorities may be the same person. Best practise to consider is for the documents to be:

- Identifiable - title, number
- Up-to-date (documents)
- Legible
- Understandable
- Logically laid out
- Clear in meaning
- Adequate
- Complete
- Self-consistent - within the purpose and scope of the system or process
- Consistent with other documents
- Available (documents)
- Retrievable (records)

Demonstrating conformance with ISO/IEC 27001

In order to claim conformity with ISO/IEC 27001, the organisation must provide evidence of the effectiveness of the ISMS.

As noted above, this may not necessarily depend on documented procedures or records, except where these are specifically required by the Standard.

Organisations, particularly small organisations, may be able to demonstrate conformity without the need for extensive documentation.

DO

Operation of the ISMS

The organisation has to plan, implement and control the processes needed to meet information security requirements, and to implement the actions arising from the planning process to meet its organisational information security objectives (Clause 8.1).

Changes must be controlled as must any actions taken to mitigate the consequences of unintended changes or any other adverse effects.

The organisation shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. This would be items such as copy machines, vending machines, production control systems (e.g. PLC) and video recording systems.

Documented information concerning the operations of the ISMS must be retained.

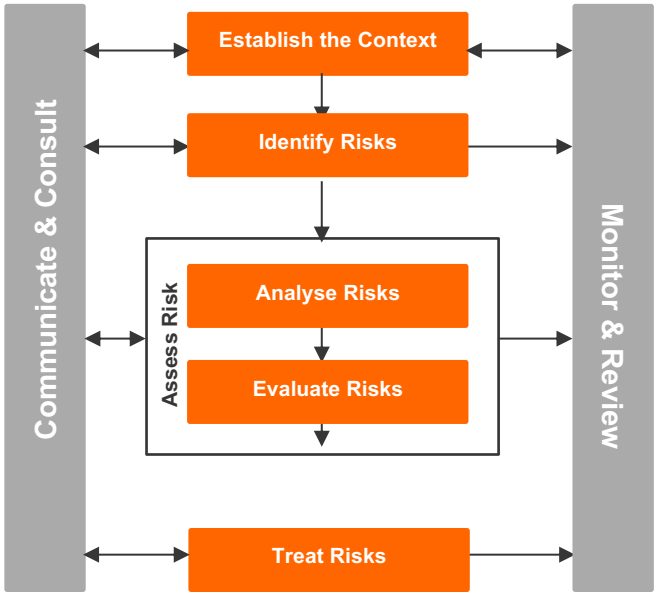
Risk assessment

Information security risk assessments must take place at planned intervals or when significant changes are proposed or occur (Clause 8.2).

The organisation will need to define and document an appropriate method for risk assessment. This is to enable the organisation to understand threats and any vulnerabilities of its critical activities and supporting resources. This must include those provided by suppliers and outsource partners.

A risk management process is shown on the following page.

Risk management process



Risk treatment (Clause 8.3)

The treatments of risks are not necessarily mutually exclusive or appropriate in all circumstances. The Auditor will need to be familiar with the options in the context of the organisation's ISMS and risk appetite in the light of the ISMS policy.

The options can include the following:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed decision.

CHECK

Performance evaluation (Clause 9)

It is the responsibility of management to monitor and review the effectiveness and efficiency of the ISMS. Management should review the appropriateness of the information security policy, scope and plans, and determine and authorise actions for correction and improvement. The requirements in Clause 9 specify how this is to be done.

Monitoring, measuring and then acting on the information received are the prime ways for ensuring that the ISMS is performing correctly and complying with the requirement for continual improvement. The retained documented information will enable an organisation to demonstrate that the system is complying with its determined processes.

The organisation must use suitable methods for monitoring ISMS processes. These methods must demonstrate the ability of processes to achieve planned results.

Auditors should have an adequate working knowledge of the key issues associated with the processes in order to be able to make a fair evaluation of the adequacy of monitoring criteria chosen.

Furthermore, they will often also need to have knowledge of the best available monitoring technologies and an understanding of their measurement characteristics and inherent accuracy / inaccuracy and / or reliability to determine the effectiveness of the processes employed.

In reality, this will be one of the prime concerns of the Auditor – seeking to ensure that the management system is effectively implemented – because effective and proactive monitoring of all elements of operation and strategy is how performance is reported for the benefit of both internal parties (self-confidence in the demonstrable capabilities of the ISMS) and external parties.

Internal audit (Clause 9.2)

The organisation must conduct internal audits at planned intervals to provide information on whether the ISMS conforms to requirements of ISO/IEC 27001 and is effectively implemented and maintained.

This means the establishment of an audit programme taking into consideration the importance of the processes concerned and the results of previous audits.

Audits must be objective and impartial and the means by which Auditors are selected must ensure that this objectivity is maintained.

Internal audit (Clause 9.2), continued

The management responsible for the area being audited must ensure that any necessary corrections and corrective actions are taken as soon as possible.

Follow-up activities will include the verification of the actions taken and the reporting of verification results.

Documented information must be available to provide evidence of the implementation of audit programmes and the audit results

Management Review (Clause 9.3)

The organisation's top management is to review ISMS, at planned intervals to ensure the continuing suitability, adequacy and effectiveness of the ISMS.

Typically, management review activities comprise a meeting to review data and issues, though a "meeting" is not required by the standard.

The review process would typically address such issues as:

- review periodicity at planned intervals;
- responsibilities;
- status of actions from previous management reviews;
- changes in external and internal issues relevant to the ISMS;
- feedback on performance and from interested parties;
- results of risk assessment and status of the risk treatment plan; and
- opportunities for continual improvement.

There must be documented information available for evidence of the results of management reviews.

Auditors can learn a great deal about management involvement and commitment by examining the results and actions emanating from the management review process.

Furthermore, because management review is a standalone, integral part of the "Plan-Do-Check-Act loop, accreditation criteria and certification bodies place great importance on this process and its results, including the completion of at least one management review prior to any certification audit.

ACT

Improvement (Clause 10)

This clause addresses the final part of the PDCA cycle; continual improvement (Clause 10.1) and nonconformity and corrective action (Clause 10.2).

First, we must define:

- Correction – "action to eliminate a detected nonconformity" (ISO/IEC 27000:2017).
- Corrective action – "action to eliminate the cause of a nonconformity and to prevent recurrence" (ISO/IEC 27000:2017).

Through the use of corrective actions to address nonconformity, the organisation is able to improve the effectiveness and efficiency of the ISMS.

Where nonconformities have occurred, the corrective action taken should be further investigated to ensure that they have been effective and have not caused other supplementary, problems to arise.

The implementation of the output of the review of the corrective actions taken should add impetus to continual improvement in the suitability, adequacy or effectiveness of the ISMS.

AUDITING FOR CONTINUAL IMPROVEMENT

To audit effectively, the Auditor will need to evaluate how the PDCA process actually contributes to the continual improvement of the ISMS. More precisely, the Auditor will need to evaluate how the monitoring and measurement processes that the organisation has established contribute to the continual improvement of the ISMS.

ISO/IEC 27001, Clause 10, requires that continual improvement to the effectiveness of the ISMS takes place through the:

- execution of the monitoring procedures;
- review of the effectiveness of the ISMS by means of the information security policy and plans;
- analysis of monitored events;
- the results of internal audits;
- management review;
- record of the actions taken.

AUDITING FOR CONTINUAL IMPROVEMENT, CONTINUED

It is the role of the Auditor to evaluate the effectiveness of these processes in ensuring that continual improvement is actually taking place.

The Auditor will need to gather information from the monitoring and review processes as evidence that the ISMS:

- ensures adequate and proportionate information security management to treat risks;
- gives confidence to customers, stakeholders and other interested parties;
- maintains and improves the competitive edge, legal compliance and commercial image.

These are the reasons that the organisation first set up an ISMS. Now, we need to know whether it is working and whether it is effective.

The audit methodology described over the rest of this course aims to provide you with the tools to do this.

ACTIVITY TWO: AUDIT EVIDENCE / AUDIT TRAIL

PURPOSE

- To develop your understanding and application of the evidenced needed to indicate that certain clauses in ISO/IEC 27001 are being implemented effectively.

TASK

- In your team, using an example of your choice, develop an audit trail that would take you through the following clauses of ISO/IEC 27001 (as a minimum):
  - Annex A.7: Physical Controls
  - Annex A.5.14 Information Transfer
  - Annex A.8: Technological Controls
  - Clause 6.1.3: Information security risk treatment
  - Clause 7.2: Competence.
  - Clause 10.2: Nonconformity and corrective action.
- Provide details of the possible audit evidence that could be available in order to verify that the clauses are being met effectively.

OUTPUT

- Be prepared to feedback your findings to the whole group.
- Learner output – Presentation.

TIME ALLOWED

- Activity: 35 minutes.
- Feedback: 35 minutes.

ACTIVITY THREE: CONTINUAL IMPROVEMENT

PURPOSE

- To consider the drivers for continual improvement in an ISMS.

TASK

- In your team, based on the requirements of ISO/IEC 27001:2022 Clause 10:
  - Produce a flowchart showing how management review might work as a process for continual improvement.
  - Consider the PDCA cycle and identify links to other clauses of ISO/IEC 27001.
  - Note: While ISO 27001:2022 does not specifically reference PDCA, Annex SL upon which it is based certainly does.

OUTPUT

- You will be asked to present your flowchart for discussion by the whole group.

TIME ALLOWED

- Activity: 40 minutes.
- Feedback: 40 minutes.

ACTIVITY FOUR: RISK TREATMENT

PURPOSE

- To provide you with the opportunity to understand risk treatment and the Statement of Applicability (SoA).

TASK

- In your team:
  - Evaluate the risk treatment plan and the SoA provided.
  - Produce a list of criticisms and/or comments.

OUTPUT

- Be prepared to discuss your response with the whole group.

TIME ALLOWED

- Activity: 40 minutes.
- Feedback: 40 minutes.

SESSION THREE

REGISTRATION, CERTIFICATION AND AUDITOR COMPETENCE

REGISTRATION, CERTIFICATION AND AUDITOR COMPETENCE

OBJECTIVES

When you have completed this session, you will be able to:

- Explain the terms used in certification and accreditation.
- Describe the certification and accreditation process.
- Understand the importance and purpose of ISO/IEC 17021.
- Distinguish between a Stage 1 and Stage 2 audit.
- Explain the purpose of surveillance visits.
- Explain the benefits of third-party certification for an ISMS for organisations and stakeholders.
- Be aware of the various Auditor certification schemes.
- Understand the competence needs of Auditors/
- Outline the content and intent of the CQI and IRCA Code of Conduct.

KEY POINTS

- Certification and registration of organisations.
- Certification of Auditors.
- Competence of Auditors.
- Personal characteristics of Auditors.
- Registration, certification and competence of Auditors.

REGISTRATION, CERTIFICATION AND AUDITOR COMPETENCE

THIRD-PARTY CERTIFICATION

There are strict rules and regulations laid down for the conduct of third-party audits that are monitored by Accreditation Bodies through the International Accreditation Forum (IAF).

In the United Kingdom, the national accrediting body is the United Kingdom Accreditation Service (UKAS) which reports directly to the Government Department of Trade and Industry. In the USA, the ANAB fulfils a similar role, as does the JAB in Japan.

The most important function of a national accreditation body is to “accredit” organisations (certification bodies) to “certificate” or “register” other organisations against National and International Standards. So UKAS accredits companies such as SGS, BSI and Lloyds to carry out audits on organisations and to register those which meet the requirements of the standard against which they are being audited.

The accreditation body will also agree the scope of accreditation with the certification body. That is the certification body will only be able to award certificates within specifically defined industrial sectors and for a specific set of standards.

ISO/IEC 17021:2015 CONFORMITY ASSESSMENT - REQUIREMENT FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF MANAGEMENT SYSTEMS

The Standard contains principles and requirements for the competence, consistency and impartiality of audits and certification of all types of management systems.

ISO/IEC 17021:2015:

- defines the principles to give confidence to all parties that a management system fulfils specified requirements;
- specifies the legal and contractual obligations of certification bodies;
- sets out the organisational management structural requirements of certification bodies;
- defines the requirements for the competence of management and staff of certification bodies;
- establishes the process requirements for conduct of certification audits;
- requires certification bodies to implement a three-year certification cycle with a recertification audit;

ISO/IEC 17021:2015 CONFORMITY ASSESSMENT - REQUIREMENT FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF MANAGEMENT SYSTEMS, CONTINUED

- requires that recertification audits and the decision on issuing new certificates must be performed prior to the expiry of the existing certificate;
- distinguishes between a Stage 1 and Stage 2 audit;
- requires corrective actions raised to address Minor nonconformities which have been raised at Stage 2 to have been reviewed and accepted (but not necessarily closed out) before a certificate of registration can be issued;
- surveillance audits in first and second years (the date of the first surveillance audit following initial certification must take place no more than 12 months from the last day of the Stage 2 audit); and
- surveillance activities to cover representative areas and functions on a regular basis and take into account any changes.

These and the other requirements relating to the audit and certification process are addressed in this manual and during the course.

The accreditation body (e.g. UKAS, ANAB, DAkkS etc) will carry out regular monitoring of the activities of the certification body against ISO/IEC 17021 and will raise nonconformity reports as appropriate.

ISO/IEC 27006 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS

ISO/IEC 27006 provides some additional requirements and guidance for certification bodies accredited to certifying organisations to ISO/IEC 17021. To achieve accreditation, the certification body must:

- have a formal, documented system of controls;
- be audited by the Accreditation Body;
- hold records on each Auditor;
- prove knowledge and experience of applicable industry sector;
- employ or have access to Auditors, including team members and technical experts to cover all of its activities.
- determine audit duration for certification audits.

CERTIFICATION PROCESS

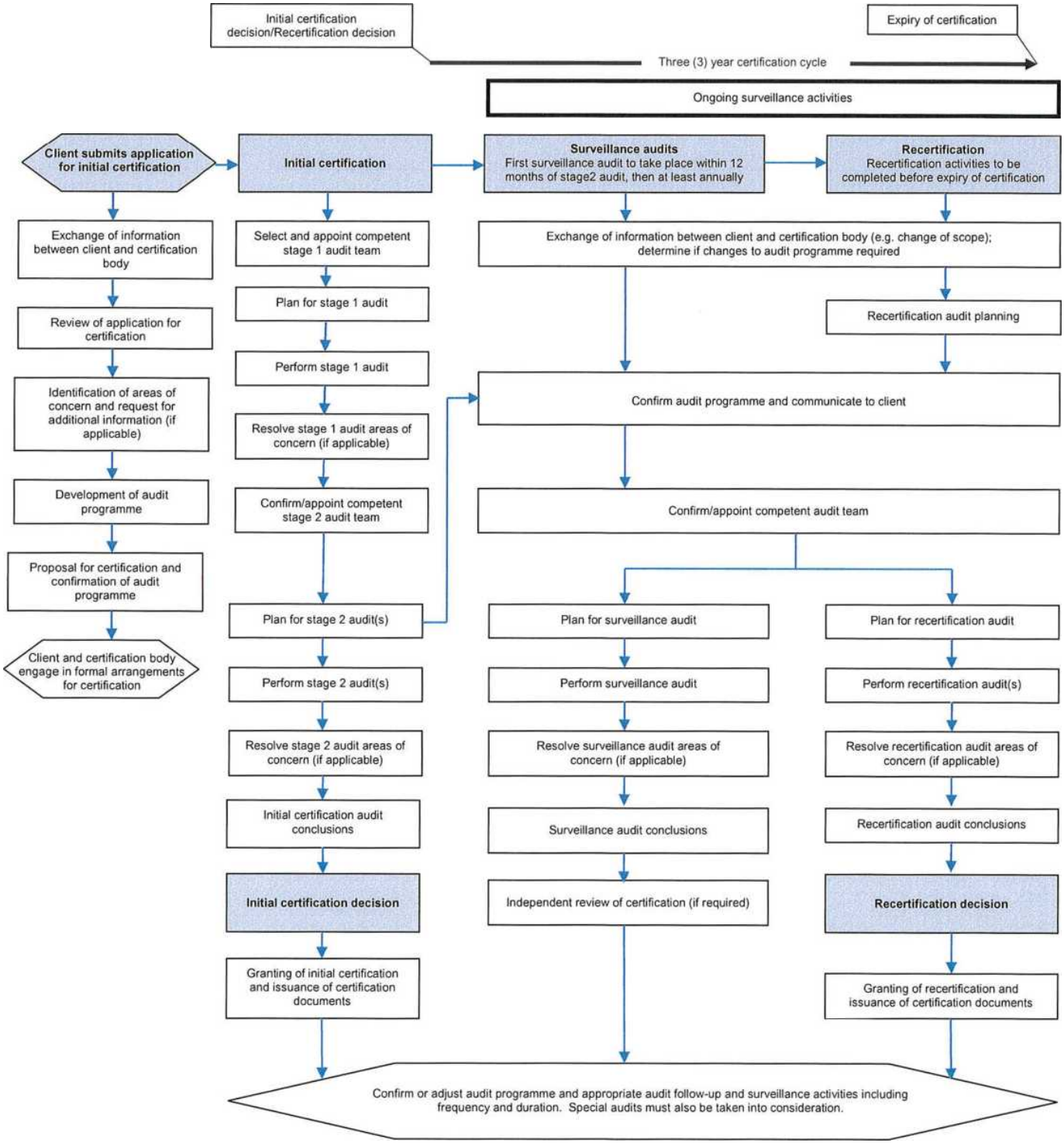
Certification of a management system provides independent demonstration that the management system of the organisation:

- conforms to specified requirements;
- is capable of consistently achieving its stated policy and objectives; and is effectively implemented.

INITIAL CERTIFICATION AUDIT

- The initial certification audit of a management system is conducted in two stages; Stage 1 and Stage 2.
- The process is shown on the next page.

Typical process flow for third-party audit and certification process



INITIAL CERTIFICATION AUDIT CONCLUSIONS

The audit team are expected to analyse all of the information and audit evidence gathered during the Stage 1 and Stage 2 audits to review the audit findings and agree on the audit conclusions.

SURVEILLANCE AUDIT

These are “mini” audits to review the ongoing effectiveness of a registered organisation’s management system. Surveillance visits take place regularly throughout the period that an organisation is registered. The duration of the audit is shorter than an initial audit and tends to be focussed on a particular part of the overall system.

A certification body is able, therefore, to look at specific processes or areas in more depth. Over the period of registration, the intention is that the whole of an organisation’s management system will have been audited in this manner.

The surveillance audit programme must include, at least:

- internal audits and management review;
- a review of actions taken on nonconformities identified during the previous audit;
- treatment of complaints;
- effectiveness of the management system with regard to:
  - achieving the certified client’s objectives;
  - progress of planned activities aimed at continual improvement;
  - continuing operational control;
  - review of any changes, and
  - use of marks and / or any reference to certification.

SURVEILLANCE AUDIT, CONTINUED

27006 reads:

9.6.2.1.2 as a minimum, every surveillance by the certification body shall review the following:

a) the effectiveness of the ISMS with regard to achieving the objectives of the client's information security policy;

b) the functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations;

c) changes to the controls determined, and resulting changes to the SoA;

d) implementation and effectiveness of controls according to the audit programme.

Surveillance audits are conducted at least once a year. The date of the first surveillance audit following initial certification shall not be more than 12 months from the certification decision date.

Surveillance visits may also form part of a supplier's audit programme.

CERTIFICATION OF AUDITORS

To ensure independence of the certification process, the organisation which certificates Auditors, is separate from that which certificates organisations.

An Auditor certification scheme is one of the means for providing consistency and accuracy in the interpretation of the Standard by Auditors.

The purpose of the Auditor Certification Scheme is to certify that an Auditor is competent, trained and qualified in the principles of auditing Information Security Management Systems against ISO/IEC 27001, and any other acceptable equivalent standards.

INTERNATIONAL SCHEMES

Examples of international schemes are those provided by:

- CQI and IRCA (Chartered Quality Institute and International Register of Certified Auditors) in the UK.
- Exemplar Global, previously RABQSA (Registrar Accreditation Board / Quality Society of Australasia) covering Australia and New Zealand;
- JAB (Japanese Accreditation Board) in Japan.

CQI AND IRCA AUDITOR CERTIFICATION SCHEME

The scheme operated by CQI and IRCA comprises five categories of ISMS Auditors:

- Principal Auditor;
- Lead Auditor;
- Auditor;
- Associate Auditor;
- Internal Auditor.

There is also an Internal ISMS Auditor certification scheme that sets the competence and integrity of persons certificated to conduct internal audits of information security systems.

Brief explanations of the categories of CQI and IRCA Auditor are included in the definitions in Appendix 1.

There are also schemes for specialist sector Auditors such as aerospace, maritime, pharmaceutical and environmental management.

To maintain and manage the scheme, CQI and IRCA:

- Sets the requirements for each grade of Auditor which focuses on an applicant's training, work, information security and audit experience.
- Approves and certificates Auditor training courses.
- Maintains records of the Continuous Professional development (CPD) of Auditors.

The CQI and IRCA certification scheme is outlined on their website (www.quality.org).

The CQI and IRCA Code of Conduct are set out overleaf.

The details of other schemes are published by the relevant Auditor certification bodies.

THE CHARTERED QUALITY INSTITUTE PROFESSIONAL CODE OF CONDUCT

For the purposes of this code “members” refers to all individuals whose competence is recognised formally by The Chartered Quality Institute [The CQI]. This includes but is not restricted to CQI members, IRCA registered Auditors and individuals on other CQI registers, as well as all members of the Board of Trustees, Advisory Council and other governance bodies.

Statement of Personal Responsibility

It is the ethical and professional responsibility of all members to demonstrate the required professional competence and behaviours in discharging the responsibilities of their role.

Members must uphold the highest ethical standards and integrity in exercising their professional duties or other activities which might impact on the reputation of the profession and of the CQI.

In support of these aims all members are expected to understand and comply with this code of conduct.

Furthermore, the CQI reserves the right to suspend or withdraw membership and all associated benefits from members who fail to comply with this code of conduct, in accordance with the Enforcement Processes detailed below.

Professional Competence and Behaviour

In recognising the values and requirements of this code of conduct members shall:

1.1. Maintain professional knowledge and competence in order to successfully undertake their role.

1.2. Act with due skill, care and diligence and with proper regard for professional standards.

1.3. Undertake appropriate continuing professional development and record it in an appropriate manner.

1.4. Ensure that clients, employers and others who may be affected by their activities are not misled or ill-informed with regard to their level of competence and capability to successfully discharge their responsibilities.

Professional Competence and Behaviour, continued

1.5. Seek appropriate support whenever they are aware that their level of competency (knowledge, skills, behaviours and experience) might be lacking with respect to the responsibilities they are assigned.

1.6. Accept responsibility and accountability for their own professional actions and decisions.

1.7. Always act in a way which supports and upholds the reputation of the Quality profession.

1.8. Work to ensure that the credibility and reputation of the CQI and all of its stakeholders is protected.

1.9. Be mindful of the distinction between acting in a personal and in a professional capacity.

1.10. When managing a team, ensure that those working for them have the appropriate level of competence, supervision and support.

1.11. Co-operate fully with the Institute in assuring the effective implementation of this Code of Conduct (including investigation and resolution of any alleged or actual breaches).

Ethical Standards and Integrity

In recognising the values and requirements of this code of conduct members shall:

2.1 Seek to establish, maintain and develop business relationships based on confidence, trust and respect.

2.2 Always act honestly in all matters relating to the Institute.

2.3 Demonstrate sensitivity for the customs, working practices, culture and personal beliefs of others.

2.4 Safeguard all confidential, commercially-sensitive and personal data acquired as a result of business relationships and not use it for personal advantage or for the benefit or detriment of third parties.

2.5 Comply with prevailing laws.

2.6 Advise the CQI Executive in writing whenever there is a suspicion that this code of conduct has been breached.

2.7 Be mindful of their responsibilities as professional people towards the wider community.

2.8 Ensure potential or known conflicts of interest are declared at the earliest opportunity to ensure professional judgement is not compromised or perceived to be compromised.

Processes for Enforcement of this Code

All members, by virtue of their association with the Institute, have agreed to abide by the following enforcement processes.

1. CQI0070 details the Misconduct Handling process for:
    a. Reporting breaches of misconduct to the CQI.
    b. Undertaking a Preliminary Investigation.
    c. Conducting a Disciplinary Hearing.
    d. Establish and acting on the Board's decision.
    e. Grounds for appeal.

2. CQI0058 details the Disciplinary Appeals process for:
    a. Submitting an appeal to the Advisory Council.
    b. Preliminary review of the appeal.
    c. Convening an appeal panel.
    d. Reviewing the appeal submission.
    e. Holding an appeal hearing.
    f. Making an appeal recommendation to the Advisory Council.
    g. Communicating the outcomes of the Appeal Panel (Preliminary Recommendation).
    h. Council review of recommendation.
    i. Appeal decision announced and actioned.

COMPETENCE OF AUDITORS

ISO 19011 sets out the desired personal behaviours and competencies needed by an Auditor.

PERSONAL ATTRIBUTES

An Auditor needs to be:

- Ethical
- Open minded
- Diplomatic
- Observant
- Perceptive
- Versatile
- Tenacious
- Decisive
- Self-reliant
- Able to act with fortitude
- Open to improvement
- Culturally sensitive
- Collaborative.

COMPETENCY

Generic knowledge and skills of management system Auditors is set out in ISO 19011

Auditors should have knowledge and skills in the areas outlined below:

- Audit principles, procedures and methods: Knowledge and skills in this area enable the Auditor to apply the appropriate principles, procedures and methods to different audits, and to ensure that audits are conducted in a consistent and systematic manner. An audit should be able to do the following:
  - apply audit principles, procedures, and methods;
  - plan and organise the work effectively;
  - conduct the audit within the agreed time schedule;
  - prioritise and focus on matters of significance;
  - collect information through effective interviewing, listening, observing and reviewing documents, records and data;
  - understand and consider the experts' opinions;
  - understand the appropriateness and consequences of using sampling techniques for auditing;

Generic knowledge and skills of management system Auditors is set out in ISO 19011, continued

- verify the relevance and accuracy of collected information;
- confirm the sufficiency and appropriateness of audit evidence to support audit findings and conclusions;
- assess those factors that may affect the reliability of the audit findings and conclusions;
- use work documents to record audit activities;
- document audit findings and prepare appropriate audit reports;
- maintain the confidentiality and security of information, data, documents and records;
- communicate effectively, orally and in writing (either personally, or through the use of interpreters and translators); and
- understand the types of risks associated with auditing.

- Management system and reference documents: Knowledge and skills in this area enable the Auditor to comprehend the audit scope and apply audit criteria, and should cover:
  - management system standards or other documents used as audit criteria;
  - the application of management system standards by the auditee and other organisations, as appropriate;
  - interaction between the components of the management system;
  - recognizing the hierarchy of reference documents;
  - application of the reference documents to different audit situations.
- Organisational context: Knowledge and skills in this area enable the Auditor to comprehend the auditee's structure, business and management practices, and should cover the following:
  - organisational types, governance, size, structure, functions and relationships;
  - general business and management concepts, processes and related terminology, including planning, budgeting and management of personnel;
  - cultural and social aspects of the auditee.

Generic knowledge and skills of management system Auditors is set out in ISO 19011, continued

- Applicable legal and contractual requirements and other requirements that apply to the auditee: Knowledge and skills in this area enable the Auditor to be aware of, and work within, the organisation's legal and contractual requirements. Knowledge and skills specific to the jurisdiction or to the auditee's activities and products should cover the following:
  - laws and regulations and their governing agencies;
  - basic legal terminology;
  - contracting and liability.

ISMS and sector-specific knowledge and skills of management system Auditors

Auditors should have the appropriate ISMS and sector-specific knowledge and skills for auditing.

It is not necessary for each Auditor in the audit team to have the same competence; however, the overall competence of the audit team needs to be sufficient to achieve the audit objectives.

The ISMS and sector-specific knowledge and skills of Auditors include the following:

- ISMS-specific management system requirements and principles, and their application;
- legal requirements relevant to the sector, such that the Auditor is aware of the requirements specific to the jurisdiction and the auditee's obligations, activities and products;
- requirements of interested parties relevant to the ISMS;
- fundamentals of information security management and the application of business and technical specific methods, techniques, processes and practices, sufficient to enable the Auditor to examine the management system and generate appropriate audit findings and conclusions;
- specific knowledge related to the particular sector, nature of operations or workplace being audited, sufficient for the Auditor to evaluate the auditee's activities, processes, and products (goods and services);
- risk management principles, methods and techniques relevant to the sector, such that the Auditor can evaluate and control the risks associated with the audit programme.

ISMS and sector-specific knowledge and skills of management system Auditors

Details and requirements on the initial and continual evaluation of Auditors and audit Team Leaders are provided in ISO/IEC 17021 and ISO 19011.

Source ISO/IEC 27001:

- 7.2.1 IS 7.2 Demonstration of Auditor knowledge and experience
  - The certification body shall demonstrate that the Auditors have knowledge and experience through:
    - **a)** recognized ISMS-specific qualifications;
    - **b)** registration as Auditor where applicable;
    - **c)** participation in ISMS training courses and attainment of relevant personal credentials;
    - **d)** up to date professional development records;
    - **e)** ISMS audits witnessed by another ISMS Auditor.
- 7.2.1.1 Selecting Auditors in addition to 7.1.2.1, the criteria for selecting Auditors shall ensure that each Auditor:
  - **a)** has professional education or training to an equivalent level of university education;
  - **b)** has at least four years full-time practical workplace experience in information technology, of which at least two years are in a role or function relating to information security;
  - **c)** has successfully completed at least five days of training, the scope of which covers ISMS audits and audit management;
  - **d)** has gained experience of auditing ISMS prior to acting as an Auditor performing ISMS audits. This experience shall be gained by performing as an Auditor-in-training monitored by an ISMS evaluator (see ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit. This experience shall be gained in at least 10 ISMS on-site audit days and performed in the last 5 years. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting.

ISMS and sector-specific knowledge and skills of management system Auditors, continued

e) has relevant and current experience;

f) keeps current knowledge and skills in information security and auditing up to date through continual professional development.

g) has competence in auditing an ISMS in accordance with ISO/IEC 27001.

- Technical experts shall comply with criteria a), b) and e).

Pre-requisite requirements for Auditors

ISO/IEC 27006 contains requirements relating to the training of certification audit teams and in particular sets out the pre-requisite level of education, work experience, Auditor training and audit experience.

Each Auditor in the ISMS audit team must:

- Have an education to the equivalent level of university education.
- Have at least four years full-time practical workplace experience in information technology, of which at least two years are in a role or function relating to information security;
- Have successfully completed five days of training, the scope of which covers ISMS audits and audit management shall be considered appropriate;
- Has gained experience of auditing ISMS prior to acting as an Auditor performing ISMS audits. This experience shall be gained by performing as an Auditor-in-training monitored by an ISMS evaluator (see ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS initial certification audit (Stage 1 and Stage 2) or re-certification and at least one surveillance audit. This experience shall be gained in at least 10 ISMS on-site audit days and performed in the last 5 years. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting. have experience which is reasonably current;
- Be able to put complex operations in a broad perspective and to understand the role of individual units in larger client organisations; and
- Keep their knowledge and skills in information security and auditing up to date through continual professional development.

SESSION FOUR

AUDITS: DEFININTION, PRINCIPLES AND TYPES

AUDITS: DEFINITION, PRINCIPLES AND TYPES

OBJECTIVES

When you have completed this session, you will be able to:

- Understand the definition of auditing.
- Explain the principles of auditing.
- Explain the purpose and differences between first, second and third-party certification audit of management systems.
- Explain the need for Auditor confidentiality.

KEY POINTS

- Audit definitions.
- Principles of auditing.
- Types of audit.

AUDITS: DEFINITION, PRINCIPLES AND TYPES

DEFINITION

ISO 19011 defines an audit as a:

> *"Systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled. "*

In other words, a check that the management system is operating effectively in accordance with the system criteria.

ISO 19011, Guidelines for auditing management systems auditing, sets out the process by which audits are conducted.

ISO 19011 contains guidance on:

- the principles of auditing;
- managing an audit programme;
- conducting an audit;
- the competence and evaluation of Auditors.

ISO/IEC 17021 Conformity assessment – Requirements for bodies providing audit and certification of management systems sets the requirements for certifications bodies to assess management systems certification bodies.

ISO/IEC 17021 contains requirements relating to:

- audit principles;
- legal and contractual matters;
- structural requirements;
- resource requirements;
- information requirements;
- process requirements;
- management system requirements.

This course is based on the requirements set in ISO/IEC 17021 and the guidelines contained within ISO 19011.

PRINCIPLES OF AUDITING

To ensure that auditing is an effective and reliable management tool, ISO 19011 contains a number of fundamental principles. Understanding and following these principles will ensure that audit conclusions are relevant and sufficient, and that Auditors working separately from one another will reach similar conclusions in similar circumstances.

AUDITING PRINCIPLES

Three of the principles relate to the personal characteristics of Auditors:

- Integrity: ISO 19011 states that this is the foundation of professionalism. Auditors must carry out their work with honesty, diligence and responsibility. They must apply and meet any legal requirements and demonstrate their competence.

  They must conduct their work in an impartial manner, remaining fair and unbiased in all of their findings. They must also be sensitive to any influences that may be exerted on their judgement when carrying out their audit. Certificated Auditors are bound by strict codes of conduct.

- Fair Presentation: This obliges Auditors to report truthfully and accurately. Audit findings, audit conclusions and audit reports reflect truthfully, accurately and completely the audit activities. Any unresolved or diverging opinions between the audit team and the auditee and any obstacles encountered are reported. Communication should be truthful, accurate objective, timely, clear and complete.

- Due Professional Care: This is the application of diligence and judgement in auditing. Auditors must exercise a degree of care appropriate to the importance of the task and to the confidence placed in them by audit clients and other interested parties. Having the necessary competence is an important part of this.

- Confidentiality: Auditors must be discreet in the use and protection of information that they acquire during an audit. This includes the handling of sensitive or confidential information. ISO 19011 requires that information should not be used for personal gain or used in any way that harms the auditee.

AUDITING PRINCIPLES, CONTINUED

Two further principles concern the audit process, namely independence and evidence-based approach (discussed below).

- Independence: Independence is the basis for the impartiality of the audit and objectivity of the audit conclusions. Auditors must be independent of the organisation or activity being audited. They must remain free from bias and conflicts of interest.
- Evidence-Based Approach: This is the rational method for reaching reliable and reproducible audit conclusions.

  Audit evidence is verifiable. It is based on samples of the information available, since the audit is conducted during a finite period of time and with finite resources.

  However, the use of sampling must be appropriate to the confidence placed in the audit conclusions.

  ISO/IEC 17021 provides a number of principles that should be applied as guidance for the decisions that may need to be made during an audit. These principles are intended to inspire confidence to all parties that a management system audit meets requirements.

  The principles are:

  - impartiality;
  - competence;
  - responsibility;
  - openness;
  - confidentiality; and
  - responsiveness to complaints.

The risk-based approach should substantially influence the planning, conducting and reporting of audits in order to ensure that audits are focused on matters that are significant for the audit client, and for achieving the audit programme objectives.

TYPES OF AUDIT

There are three types of audit:

- First-party (internal audit)
- Second-party (external audit)
- Third-party (external audit)

FIRST PARTY (INTERNAL AUDIT)

- Definition:
  - An audit by the organisation of its own systems and procedures.
- Objective:
  - To assure maintenance, development and improvement of the ISMS.
- Requirement:
  - ISO/IEC 27001, Clause 9.2.

Use of the internal ISMS audit by Auditors conducting certification audits

Certification bodies have always issued certificates with the understanding that they signify organisations' competence to effectively manage their own affairs, (rather than the certification body overseeing every last detail of a system). Since effective internal auditing has long been recognised as an integral component of effective system management, the certification Auditor will evaluate the internal ISMS audit arrangements and results to determine their effectiveness.

In other words, a certification Auditor can, (and indeed, should) as a direct result of the findings and opportunities for improvement concerning the effectiveness of an organisation's internal audit system, amend the planning for an audit to suit these findings.

The Auditor may obtain information during the Stage 1 audit. For example, if the Stage 1 audit had revealed that the organisation's audit staff had not adequately audited certain key operations within the organisation during previous audits, the certification Auditor would "plan-in" these operations during the Stage 2 audit in order to ensure that these were "controlled".

Of course, the converse could apply; sampling could be reduced if the internal audit system demonstrated complete and thorough auditing of certain operations.

Use of the internal ISMS audit by Auditors conducting certification audits, continued

Essentially, a certification Auditor needs to determine whether the audit programme(s) and methodology is based upon the:

- current policy, objectives and targets of the organisation;
- current management programmes of the organisation;
- operational controls of the organisation.

In order to be able to do this, it is essential for the certification Auditor to be completely briefed in the scope and application of the ISMS of the organisation to maintain a constant "point of reference" for questioning.

The certification Auditor also needs knowledge of the policy and objectives and targets as a further “point of reference” during the review of internal audit performance.

Certain key principles should apply no matter what organisation circumstances apply.

Examine the training of Internal Auditors – is it adequate in:

- Approach to the organisation’s information security issues?
- "Grounding" in audit methodology?

Examine the audit programme – is it:

- Comprehensive in its coverage of the system?
- Capable of change if circumstances dictate?
- Demonstrating that previous audit findings are used?
- Relevant to the critical aspects of the organisation?

Examine the audit planning and preparation – is it:

- Demonstrating allocation of trained Auditors with impartiality and objectivity?
- Demonstrating use of checklists prepared to evaluate the system, not just the standard?

Examine the audit results – do they:

- Document the complete audit activity, recording "good" and "bad"? The results should include the comprehensive recording of evidence.
- Demonstrate that Auditor training was effective?

Use of the internal ISMS audit by Auditors conducting certification audits, continued

Examine the finding statements / CAR's – do they:

- Comply with any classification criteria identified?
- Demonstrate that Auditor training was effective?
- Form a basis from which corrective action can be taken?
- Demonstrate effective review of successful implementation of corrective actions and "timely" preventative measures being achieved?

Examine the audit reports – do they:

- Provide an adequate tool for top management's further review on the basis of determining improvement and system effectiveness?

All of these principles require that the internal audits by an organisation must focus on the ISMS and the activities controlling service levels.

By implication, this also means that an organisation must ensure that the personnel used for internal audits are trained in the information security related issues in the areas / activities they will be responsible for auditing.

Otherwise, it is unlikely that the Internal Auditor will be able to adequately judge effectiveness.

SECOND PARTY (EXTERNAL AUDIT)

- Definition:
  - An audit by the organisation on its suppliers and sub-contractors (or an audit on the organisation by its customers / clients).
- Objective:
  - To determine the suitability of suppliers; and
  - Appraise supplier / sub-contractor performance in respect of information security management.

THIRD PARTY CERTIFICATION AUDIT (EXTERNAL AUDIT)

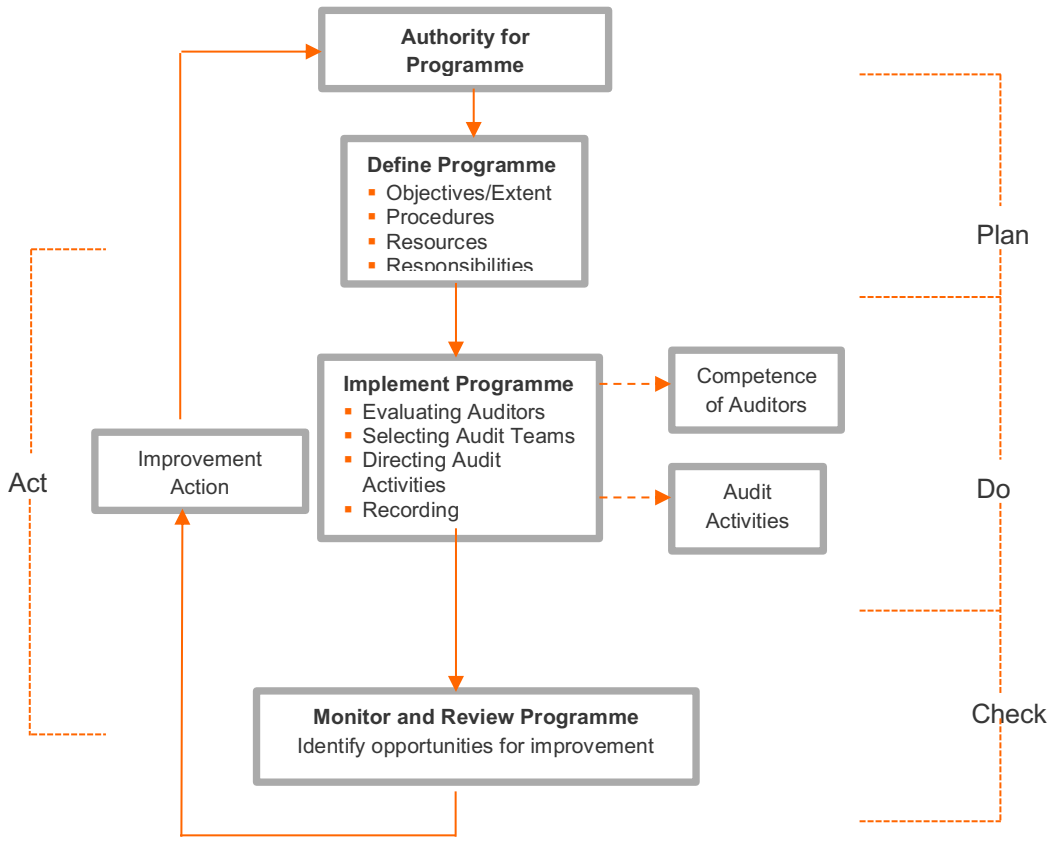
- Definition:
  - Audit carried out by an auditing organisation independent of the client and the parties that rely on certification, for the purpose of certifying the client's management system (ISO/I EC 17021).
- Objective:
  - To determine whether an organisation's ISMS has been established, documented, implemented and maintained in accordance with a specified standard.

AUDIT PROGRAMMES

For any organisation, audit programmes must be determined, managed and controlled in order to be effective and to demonstrate continual improvement.

The diagram below shows the management of an audit programme related to the Plan-Do-Check-Act cycle.

The management of an audit programme



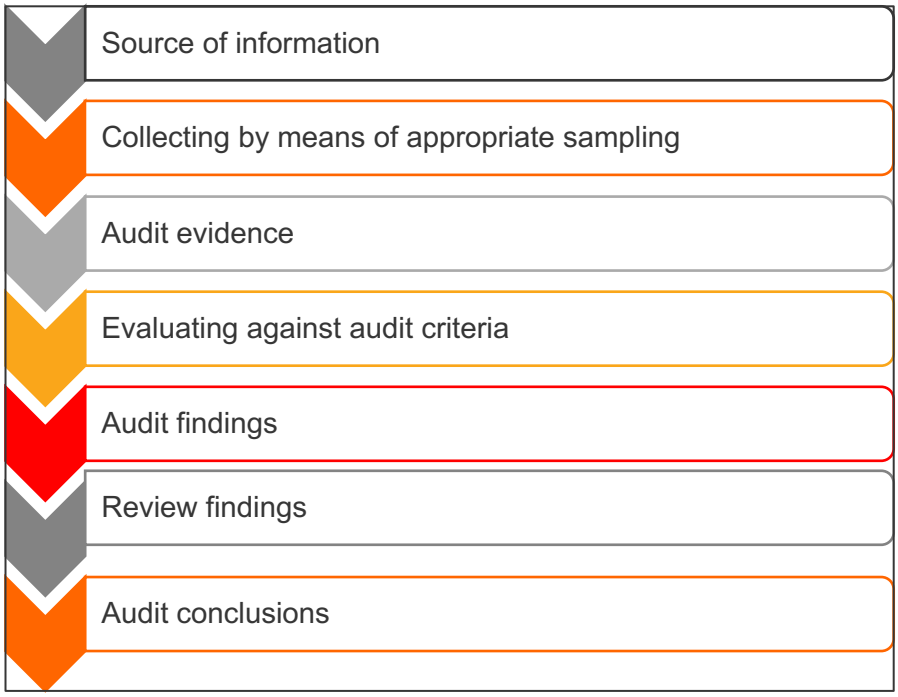
AUDIT PROGRAMMES, CONTINUED

Examples of audit programmes include:

- A series of internal audits covering an organisation-wide ISMS.
- A three-year cycle of certification / registration and surveillance audits conducted by a third-party certification body / registrar on an information security management system.
- Second-party evaluations of potential suppliers.

This diagram below shows an overview of the audit process of collecting and verifying from ISO 19011.

Collecting and verifying information



Appendix 2 contains a possible pro-forma for an internal audit programme.

PRE-AUDIT VISITS (GAP ANALYSIS)

THE PURPOSE AND BENEFITS OF A PRE-AUDIT VISIT

In some instances, a pre-audit visit by the Lead Auditor and/or the audit team may take place.

This is outside of the certification Stage 1 and Stage 2 audit process and, where undertaken, focuses on the elements and requirements of the management system to identify any gaps or shortfalls that may exist so that these can be addressed before the formal audit begins.

SESSION FIVE

THE AUDIT PROCESS

THE AUDIT PROCESS

OBJECTIVES

When you have completed this session, you will be able to:

- Determine the audit objectives, the purpose and significance of the audit scope and criteria.
- Understand resourcing of the audit, the importance of the Auditor and team competency and the selection of team members.
- Outline the different audit methods, including on-site and remote audit activities and audit activities requiring human interaction and non-human interaction.
- Describe the roles and responsibilities of the audit client, Auditors, Lead Auditors, Guides and Observers.

KEY POINTS

- Certification process.
- Planning the audit.
- Audit roles and responsibilities.
- Good practice at meetings.

THE AUDIT PROCESS

GENERAL

CERTIFICATION AUDIT

There are a number of distinct activities that take place during a certification audit.

These form an audit programme and include:

- A two-stage initial audit.
- Surveillance audits in the first and second year; and
- A re-certification audit in the third year before the expiration date of the certificate.

SECOND-PARTY AUDIT

Some second-party audits may go through a similar two-stage process; others may be less structured depending on the requirements of the contract and the complexity of system being audited.

FIRST-PARTY AUDIT

Generally, internal audits are not so formally structured and the requirements for these audits are set out in the clause of the standard concerning Internal Audits.

COURSE STRUCTURE

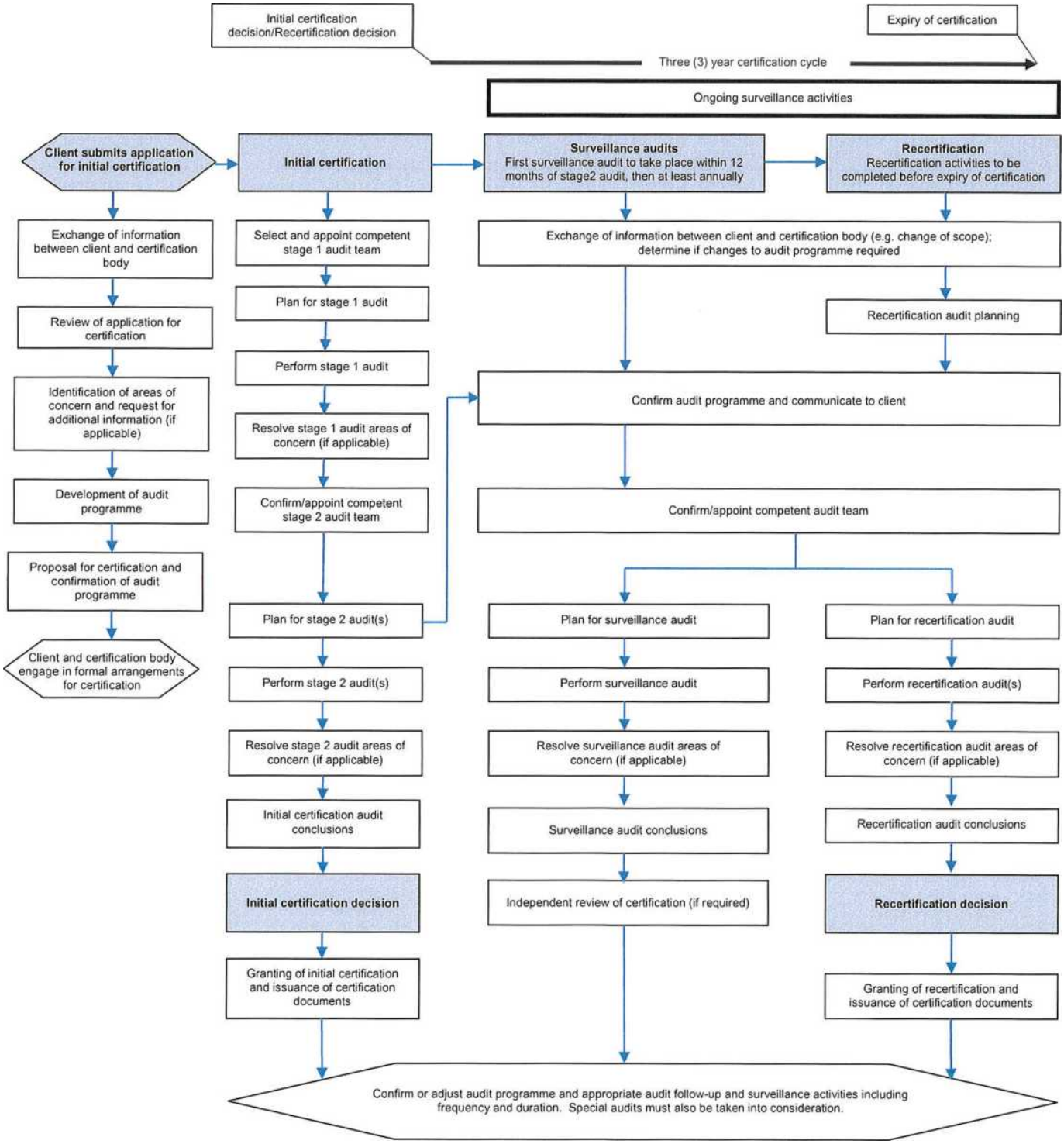
This course follows the structure of an initial certification audit, differences in approach between this and other audits will be addressed where appropriate.

The areas covered are:

- Audit planning.
- Stage 1 audit; and
- Stage 2 audit.

On the next page, taken from ISO/IEC 17021, is the diagram covered earlier which shows a “typical process flow for third-party audit and certification process”.

Typical process flow for audit and certification process



PLANNING THE AUDIT

GENERAL

For an initial certification audit, the planning process will begin with the receipt of an application from an audit client. For a second-party audit this planning process may be initiated through the tender process or before a contract is awarded or as part of an on-going contract. An internal audit programme will be planned taking into consideration the status and importance of the processes and areas to be audited as well as the results of previous audits.

AUDIT OBJECTIVES

Within the overall audit programme, each individual audit should be based on documented objectives, scope and criteria.

The objectives of an audit may include one or all of the following:

- confirming that the management system complies with all the elements of the 'standard';
- determining as to whether the management system is designed to achieve and is achieving, regulatory compliance and continual improvement of in the performance of the system processes;
- confirming that the organisation complies with its own policies and procedures;
- evaluating the capability of the management system to ensure compliance with legislative and contractual requirements;
- evaluating the effectiveness of the implemented management system in meeting specified objectives; and
- identifying areas of potential improvement of the management system.

AUDIT SCOPE

The audit scope describes the extent and boundaries of the audit in terms of factors such as:

- physical locations;
- organisational units and / or outsourcing;
- products, activities and processes to be audited; and
- the duration of the audit.

THE AUDIT CRITERIA

The audit criteria may include as applicable:

- the requirements of the management system standard e.g. ISO/IEC 27001;
- policies;
- procedures / SOPs;
- regulations, legislation;
- specific management system requirements;
- contract requirements; and
- industry sector codes of conduct.

THE AUDIT OBJECTIVES, SCOPE AND CRITERIA

These should be defined by the organisation being audited.

As a consequence, any subsequent changes to these need to be agreed with the client, audit programme management, and if appropriate, the auditee, after consultation with the Auditor.

AUDIT TIME AND AUDIT STAGES

ISO 17021 sets out points that should be considered in the allocation of time for the initial audit (divided in Stage 1 and Stage 2 audits, surveillance audits and recertification audits). Factors include:

- the size of the ISMS scope (e.g. number of information systems used, number of employees);
- complexity of the ISMS (e.g. criticality of information systems, risk situation of the ISMS);
- the type(s) of business performed within scope of the ISMS;
- extent and diversity of technology utilised in the implementation of the various components of the ISMS (such as the implemented controls, documentation and / or process control, corrective / preventive action etc.);
- number of sites;
- previously demonstrated performance of the ISMS;

AUDIT TIME AND AUDIT STAGES, CONTINUED

- extent of outsourcing and third-party arrangements used within the scope of the ISMS;
- the standards and regulations which apply to the certification.

Certification bodies must be prepared to substantiate or justify the amount of time used in any initial audit, surveillance audits and recertification audit.

MULTI-SITE SAMPLING

For a large client with several or many sites it may be appropriate to sample sites covering the same activity in various locations. The rationale for the sampling plan shall be documented for each client.

REMOTE AUDITING

The availability of information and communication technologies may be used to conduct all or some of the audit remotely; for example, by video conferencing, the observation of work by means of surveillance cameras and the completion of questionnaires as well as on-line reviews and checks.

Remote audits will be performed at any place other than at the location of the auditee and irrespective of the distances involved. The feasibility of this method will depend on the level of confidence that exists between the Auditor and the audit client or auditee. Remote auditing also refers to activities that are conducted off-site such as the document review, the completion of checklists and the analysis of data.

INTERACTIVE AND NON-INTERACTIVE AUDIT ACTIVITIES

Interactive audit activities involve human interaction; i.e.; interaction between the audit client's personnel and the audit team. Examples include interviews, completing checklists and questionnaires with auditee participation.

Non-interactive audit activities are those where there is no human interaction between the auditee and the audit team; for example, the review of documents and sampling of products, equipment, facilities and documentation and on-line checks. Most audits will be made up of a mix of interactive and non-interactive activities.

THE AUDIT TEAM

AUDIT TEAM SELECTION

As soon as the audit has been declared feasible, the composition of the audit team should be established. The CB Audit Programme Manager should appoint an audit team leader with the appropriate skills and competence needed to achieve the objectives of the audit.

The audit team will comprise an audit Team Leader and may comprise Auditors, Auditors-in-training and technical experts, working under the direction of the audit Team Leader. However, if there is only one Auditor, that Auditor should perform all of the duties of the audit team leader.

Consideration should be given to the following issues when deciding the size and composition of the audit team:

- audit objectives, scope, criteria, location(s) and estimated duration (Stage 1 and Stage 2 audits);
- whether the audit is a combined, integrated or joint audit;
- the overall competence needed to achieve audit objectives;
- requirements of accreditation or certification bodies as appropriate;
- the language of the audit and understanding of the auditee's social and cultural environment;
- the need to assure the independence of the audit team from the activities to be audited and to avoid any conflicts of interest;
- the ability of the audit team members to interact effectively with the auditee and to work together.

The audit client and the individual auditee have the right to request the replacement of particular team members on reasonable grounds that should be made to the audit programme management. Examples of reasonable grounds may be those of conflicting interests (such as an audit team member was former employee of the auditee or provided consultancy services) or previous unethical behaviour.

The selected team Auditors must have an understanding of the sector of business in which they are auditing and of the key issues for the organisation. They should be aware of the culture and ethics of the organisation to be audited. This is important when evaluating the pro-active role of management integration of business objectives, policy, and ISMS requirements.

AUDITOR ROLES AND RESPONSIBILITIES

Team Leader knowledge and skills

The audit team leader should have the knowledge and skills and provide leadership to the audit team, in order to facilitate the efficient and effective conduct of the audit.

An audit team leader should have the knowledge and skills necessary to do the following:

- balance the strengths and weaknesses of the individual audit team members;
- develop a harmonious working relationship among the audit team;
- manage the audit process, including:
  - planning the audit and making effective use of resources during the audit;
  - managing the uncertainty of achieving audit objectives;
  - protecting the health and safety of the audit team members during the audit, including ensuring compliance of the Auditors with the relevant health, safety and security requirements;
  - organizing and directing the audit team members;
  - providing direction and guidance to Auditors-in-training;
  - preventing and resolving conflicts, as necessary;
  - communication with the audit client.
- represent the audit team in communications with the person managing the audit programme, audit client and auditee;
- lead the audit team to reach the audit conclusions;
- prepare and complete the audit report.

In addition, ISO/IEC 27006 requires that audit team leaders have:

- knowledge and skills to manage the certification audit process;
- been an Auditor in at least three complete ISMS audits;
- demonstrated the capability to communicate effectively, both orally and in writing.

Audit team tasks

The audit team leader should assign to each team member responsibility for auditing specific management system processes, functions, sites, areas and activities.

Such assignments should take into account the need to maintain Auditor independence, competence and efficient use of resources.

The allocation of tasks must be made known the organisation being audited. The audit team will:

- examine and verify the structure, policies, processes, procedures, records and related documents of the organisation relevant to the management system;
- determine that these meets all of the requirements relevant to the intended scope of certification;
- determine that the processes and procedures are established, implemented and maintained effectively, to provide a basis for confidence in the auditee's management system; and
- communicate to the auditee, for action, any inconsistencies between the policy, objectives and targets, and the results.

Responsibilities of team members

Team members should:

- review all relevant information related to their assigned tasks;
- prepare any work documents (including checklists) necessary to carry out those tasks;
- comply with the audit requirements;
- carry out assigned duties effectively and efficiently;
- report nonconformities and audit findings to the team leader;
- co-operate and support the team leader.

Responsibilities of team members, continued

During any audit, team members should:

- stay within the audit scope;
- communicate the audit requirements to the auditee;
- collate the evidence from the audit both for and against conformity;
- document any Corrective Action Requests (CARs);
- report the audit findings to the auditee;
- verify corrective actions taken in response to CARs; and
- retain and safeguard all documents pertaining to the audit.

Communication during the audit

During the audit, the audit team must assess audit progress and exchange information. The team leader may need to reassign work as needed between the audit team members and periodically communicate the progress of the audit and any concerns to the auditee.

Should the team uncover evidence that indicates that the audit objectives cannot be met or suggests the presence of an immediate and significant risk to the integrity of the organisation's ISMS, the team leader must report this to the auditee client. Appropriate action must be taken which may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit.

The team leader must review with the client any need for changes to the audit scope which becomes apparent as on-site auditing activities progress.

Observers and Guides

- Observers

  The presence and justification of Observers during an audit activity must be agreed with the team leader and the auditee before the conduct of the audit.

  The audit team must ensure that Observers do not influence or interfere in the audit process or outcome of the audit. Observers may include members of the auditee organisation, consultants, witnessing accreditation body personnel, regulators or other justified persons.

Observers and Guides, continued

- Observers (continued)

  In relation to the presence of consultants during a certification or surveillance audit it is up to the Lead Auditor and the audit to team to ensure that they set the boundaries in the opening meeting to ensure that the consultant will only act as an Observer.

  The consultant is not the one responsible for controlling the system of the site on a day to day basis. The audit is an assessment of 'understanding and ownership' of the client and the organisation and the actual level of compliance reflected from the client and their management system is the critical element of the audit.

  If the consultant is involved it adds doubt to the level of control the site will have for the following 12 months until the next audit. The purpose of the audit is to determine the organisation's ability to successfully operate its own information security management system so it is important that the participation of a systems consultant must not interfere or prejudice this.

  If the consultant coaches company staff during the audit this may be interpreted as inadequate understanding and ownership of the system by the company and potentially distort the result of the audit.

- Guides

  On all third- and second-party audits, each Auditor must be accompanied by a guide, unless otherwise agreed to by the audit team leader and the client. Guide(s) are assigned to the audit team to facilitate the audit. It is the responsibility of the audit team to ensure that Guides do not influence or interfere in the audit process or outcome of the audit.

  - The responsibilities of a guide can include:
  - establishing contacts and timing for interviews;
  - arranging visits to specific parts of the site or organisation;
  - ensuring that rules concerning site safety and security procedures are known and respected by the audit team members;
  - witnessing the audit on behalf of the client; and
  - providing clarification or information as requested by an Auditor.

GOOD PRACTICE AT MEETINGS

At meetings, Auditors should remain polite, calm and professional at all times.

They should:

- introduce themselves;
- ensure that the agenda is known and understood;
- keep to the agenda;
- keep control;
- keep to time;
- avoid arguments;
- listen to others; and
- maintain appropriate records.

ACTIVITY FIVE: ISMS AUDIT QUESTIONNAIRE

PURPOSE

- To develop your understanding and application of the requirements of the ISMS.

TASK

- In the questionnaire provided on the following page, analyse the statements provided and indicate whether you consider the statements to be ***'True'*** or ***'False'***.
- If you consider the statements to be ***'True'***, please indicate the relevant clause/Annex number from ISO/IEC 27001 that supports your decision.

OUTPUT

- All learners are expected to contribute to the discussion.
- Present your findings to the whole class.

TIME ALLOWED

- Activity: 45 minutes.
- Feedback: 45 minutes.

ISMS AUDIT QUESTIONNAIRE

NO.	STATEMENT	TRUE (T) / FALSE (F)
1)	Since the Accounting department is not exposed to any information security risk, they are not part of the ISMS.	
2)	There must be a procedure setting out how to control risks.	
3)	Part of the responsibility of a risk owner is to accept any residual risks to information security.	
4)	Any information security system must reflect the requirements of ISO/IEC 27001.	
5)	The security policy must be clearly displayed on all notice boards.	
6)	Criminal and civil law lie outside the responsibility of the organisation and, therefore, do not have to be addressed by the ISMS.	
7)	The organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes.	
8)	There can be no exclusions to any of the clauses in ISO/IEC 27001.	
9)	All of the documents in the ISMS must be listed.	
10)	Personnel of the organisation and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function.	
11)	ISO/IEC 27001 can be used by internal and external parties to assess the organisation's ability to meet the organization’s own information security requirements.	
12)	Organisations must assess the potential consequences that would result if the risks identified related to associated with the loss of confidentiality, integrity and availability were to materialise.	
13)	The reason that some controls are not addressed must be given in the Statement of Applicability (SoA).	

NO.	STATEMENT	TRUE/FALSE
14)	Regardless whether a control from Annex is included in the Statement of Applicability (SoA) or not, justification must be provided	
15)	The setting of measurable information security objectives is the job of management.	
16)	Documentation produced by outside agencies such as standards, regulations and so on, cannot be part of the ISMS.	
17)	The information security policy must be signed by the Chief Executive.	
18)	All information security documents will need to be translated into all of the languages that are spoken by the workforce.	
19)	Procedures for preventive action must be clearly defined.	
20)	The requirements of the Standard do not set out exactly how the system should be designed.	
21)	The organisation shall determine: a) interested parties that are relevant to the information security management system.	
22)	The organisation shall determine the boundaries and applicability of the information security management system to establish its scope.	
23)	The scope of the ISMS is always the entire company.	
24)	Top management shall ensure that the resources needed for the information security management system are available.	
25)	The organisation shall define and apply an information security risk treatment process	
26)	When the organisation determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.	
27)	When a nonconformity occurs, the organisation shall determine the causes of the nonconformity.	
28)	When a nonconformity occurs, the organisation shall determine if similar nonconformities exist, or could potentially occur.	

NO.	STATEMENT	TRUE/FALSE
29)	When a nonconformity occurs, the organisation shall review the effectiveness of any corrective action taken.	
Annex A controls are not always applicable to a particular organisation as they can be excluded, however they are in the normative Annex A. The organisation still needs to review these and provide a "justification" for inclusion or exclusion from the statement of applicability.		
30)	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	
31)	The organisation shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	
32)	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.	
33)	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	
34)	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements	
35)	Access to external websites shall be managed to reduce exposure to malicious content.	

SESSION SIX

PREPARING FOR THE ON-SITE AUDIT (AUDIT STAGE 1)

PEPARING FOR THE ON-SITE AUDIT (AUDIT STAGE 1)

OBJECTIVES

When you have completed this session, you will be able to:

- Explain the purpose of a Stage 1 audit, including the document review, and describe a typical Stage 1 audit process and outputs.
- Determine the duration of an audit.
- Prepare an audit plan.

KEY POINTS

- Initial contact with the auditee.
- Stage 1 audit.
- Document review.
- The audit plan.
- Work documents.

PREPARING FOR THE ON-SITE AUDIT (AUDIT STAGE 1)

INITIAL CERTIFICATION AUDIT

The audit process begins with the application by the client to the Certification Body.

APPLICATION

A certification audit application will be received by the Certification Body from the organisation wishing to be certified.

The application will contain information concerning:

- the scope of the certification;
- the general features of the organisation;
- general information such as activities, human and technical resources, functions and relationship in a larger corporation, if any;
- information concerning all outsourced processes;
- the standards or other requirements for which the organisation is seeking certification; and
- information concerning the use of consultancy relating to the management system.

Before proceeding with the audit, the Certification Body will review the application and supplementary information for certification to ensure that the information about the applicant organisation and its management system is sufficient for the conduct of the audit.

Assuming that the certification body goes ahead with the audit, the Certification Body shall determine the competences it needs to include in its audit team and for the certification decision.

INITIAL CONTACT WITH THE AUDITEE

The initial contact with the auditee may be formal or informal:

- establish communication channels;
- provide information on proposed timings;
- obtain information for selecting the audit team i.e. scope and products, number of locations etc.;
- request documentation and records; and
- make arrangements for the audit.

The need for accompanying persons such as Observers, Interpreters, Technical Experts or Guides for the audit team should be mutually agreed. The need for accompanying persons such as Observers, Interpreters or Guides for the audit team should be mutually agreed.

FEASIBILITY OF THE AUDIT

At this point, the formal audit process will begin with the decision as to the feasibility of the audit. The Certification Body should determine the feasibility of the audit, taking into consideration such factors as:

- sufficient and appropriate information for planning the audit;
- business objectives, policies, products;
- adequate co-operation from the audit client; and
- availability of time and adequate resources.

Once the entire information gathering is complete and decisions have been made, the client can be presented with an accurate proposal of costs and plan of action. Subject to contractual agreement, the audit is then scheduled with the client.

Where the audit is not feasible, an alternative should be proposed to the audit client by the audit programme manager, in consultation with the audit client.

The feasibility of the audit should be reviewed after Stage 1 audit has been completed, taking into account anything that had been identified during Stage 1.

STAGE 1 AUDIT

PURPOSE OF THE STAGE 1 AUDIT

ISO/IEC 17021 sets out the function of the Stage 1 Audit:

- audit the client's management system documentation;
- evaluate the client's location and site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for the stage 2 audit;
- review the client's status and understanding regarding requirements of the standard, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the management system;
- collect necessary information regarding the scope of the management system, processes and location(s) of the client, and related statutory and regulatory aspects and compliance (e.g. quality, environmental, legal aspects of the client's operation, associated risks, etc.);
- review the allocation of resources for Stage 2 audit and agree with the client on the details of the Stage 2 audit;
- provide a focus for planning the Stage 2 audit by gaining a sufficient understanding of the client's management system and site operations in the context of possible significant aspects;
- evaluate if the internal audits and management review are being planned and performed, and that the level of implementation of the management system substantiates that the client is ready for the Stage 2 audit.

For most management systems, ISO/IEC 17021 recommends that at least part of the Stage 1 Audit be carried out at the client's premises in order to achieve the objectives stated above.

Stage 1 audit findings are documented and sent to the client. These should include the notification of any areas of concern that could be classified as nonconformity during the Stage 2 audit. Stage 1 audit findings are documented and sent to the client.

These should include the notification of any areas of concern that could be classified as nonconformity during the Stage 2 audit.

PLANNING THE STAGE 1 AUDIT

The team leader has to acquire some basic information before determining his/her ability to perform a Stage 1 audit, and the resources needed. As noted above, this is normally done through the application and/or a questionnaire that will provide information concerning:

- process or industry skills needed;
- legislative knowledge required;
- management system experience required;
- number of Auditors required;
- number of days required.

The team leader can then identify:

- the necessary skills needed;
- if the client organisation's activity falls within an existing accredited scope of operation.

DOCUMENT REVIEW

The next stage in the preparation process is for the Auditor (the audit team leader or by an Auditor nominated by the audit team leader) to study the documents relevant to the audit criteria, objectives and scope of the audit.

This is called the document review or "desk study" or documentation audit.

The purpose of the review is to provide information to the Auditor for the on-site audit activities.

The Auditor will need to satisfy themselves that the management system as described in the documented processes meets the requirements of the audit criteria.

For an initial certification, the audit criteria will be requirements of the relevant standard.

In undertaking the review, the Auditor will consider whether the system and the processes referenced within the system are appropriate to the needs of the business.

Once satisfied that the system and processes are adequately described, documented and meet the requirements of the relevant standard, the Auditor should use this information to:

- devise an audit plan to notify the auditee of the format for the audit; and
- develop the necessary working documents for the audit;

DOCUMENT REVIEW, CONTINUED

Depending on the type of audit, and the objectives and scope of the audit, the Auditor will wish to review:

- the documented statements of policy and objectives;
- the documented procedures;
- other documents needed by the organisation so as to gain a thorough understanding of the organisation and its processes, these may include:
  - operational procedures; and
  - work instructions.
- records.

In an internal audit, the Auditor will probably concentrate on the documentation (procedures or work instructions) covering the precise scope of the audit.

The documentation should be reviewed to determine the conformity with the audit criteria. The outcome of the document review on an initial certification audit will be contained in a Stage 1 Audit Report.

CONCERNS AT STAGE 1

Stage 1 audit findings are documented and sent to the client. These should include the notification of any areas of concern that could be classified as nonconformity during the Stage 2 audit.

ISO/IEC 17021, Clause 9.3.1.2.4 does mention that:

“In determining the interval between stage 1 and stage 2, consideration shall be given to the needs of the client.”

The audit should not continue until the deficiencies are resolved to the satisfaction of the audit programme management in consultation with the audit client, the audit team leader and, if appropriate, the auditee.

WORK DOCUMENTS

Work documents are those used by the audit team for the purpose of reference and/or recording the audit. They can include:

- audit procedures, checklists and sampling plans;
- the audit plan;
- checklists, for recording information and supporting evidence;
- records of meetings; and
- forms for reporting nonconformities and audit findings.

The use of these documents, such as audit plans, checklists and forms, should not restrict the extent of audit activities.

Work documents should be retained, at least until audit completion. Audit team members should suitably safeguard those involving confidential or proprietary information.

DETERMINING AUDIT TIME

The audit duration will need to be determined and will be affected by (consider ISO/IEC 27006):

- the requirements of the relevant management system standard;
- the size and complexity of the audit client and their processes;
- the technological and regulatory context;
- whether there is any outsourcing of any activities included in the scope of the management system;
- the results of any previous audits;
- the number of sites and multi-site considerations;
- the risks associated with the products, processes or activities of the organisation;
- whether the audit is combined, joint or integrated.

THE AUDIT PLAN

The audit team leader should prepare a plan for the on-site audit activities. The plan should provide the necessary information to the audit team, auditee and audit client.

It should enable the scheduling and co-ordination of the audit activities. An example of an audit plan pro-forma below and also in Appendix 3.

The level of detail should be adapted to suit the scope and complexity of the audit. The details may differ between initial and surveillance audits and between internal and external audits.

In developing the plan, the audit team leader should consider the:

- appropriate sampling techniques;
- composition of the audit team and its collective competence;
- risks to the organisation created by the audit; for example, accessing company information remotely or online.

The audit plan should include the:

- audit objectives and scope;
- audit criteria and reference documents;
- dates and places where the on-site audit activities are to be conducted;
- identification of the organisational and functional units and processes to be audited;
- expected time and duration for audit on-site activities, including meetings with the auditee's management and audit team meetings.

The plan may also include, as appropriate:

- the identification of the sites, activities and management system processes that are essential to meeting audit objectives in order to allocate appropriate resources to critical areas of the audit;
- the identification of the auditee's key representatives participating in the audit;
- the working and reporting language(s) of the audit where this is different from the language of the Auditor(s) and/or the auditee;
- the identification of roles and responsibilities of the audit team members and any accompanying persons;

THE AUDIT PLAN, CONTINUED

- the audit report topics (including any methods of non-conformity classifications), format and structure, expected date of issue and distribution;
- logistic arrangements (travel, on-site facilities, etc.);
- matters related to confidentiality;
- any arrangements for audit follow-up actions.

An example of an audit plan or itinerary is shown on the following page.

In planning on-site audits, Auditors need to be aware of, and take into consideration, any local customs or cultural issues that may have a bearing on the conduct of the audit.

These may relate to language, dress code and personal conduct of the Auditor. Auditors must be sensitive to the needs and expectations of auditees.

The plan should be reviewed and accepted by the audit client and presented to the auditee before the audit.

Any objections by the auditee should be resolved between the audit team leader, the auditee and the audit client before continuing the audit.

The audit plan should be sufficiently flexible to permit changes, such as any changes in emphasis that may become necessary as the on-site audit activities progress. Any revised audit itinerary should be agreed between the parties concerned before continuing the audit.

EXAMPLE OF AN AUDIT PLAN PRO-FORMA

Organisation:			
Address:		**Date(s) On-site:**	
Lead Auditor:			
Team Member(s):			
Standard(s):			
Audit Language:			
Audit Scope and Observations:			
Criteria and Reference Docs:			

Date	Time	Auditor	Area / Department / Process / Function	Key Contact

Notes:

- Times are approximate and will be confirmed at the opening meeting prior to commencement of the audit.
- Auditors reserve the right to change, or add to the elements listed before, or during the audit depending on the results of on-site investigation.
- A private place for preparation, review and conferencing is requested for the Auditor's use.
- Please provide a light working lunch on-site each audit day.

ACTIVITY SIX: DOCUMENT REVIEW

PURPOSE

- To provide you with the opportunity to review ISMS documentation and determine whether the organisation is meeting its own ISMS obligations and the requirements of ISO/IEC 27001.

TASK

- In your team:
  - Review the ISMS documents provided.
  - Determine whether the organisation is meeting its own ISMS obligations and the requirements of ISO/IEC 27001, and
  - Produce a list of any comments or criticisms.

OUTPUT

- Be prepared to feedback your findings to the whole group.
- Learner output – Presentation.

TIME ALLOWED

- Activity: 45 minutes.
- Feedback: 45 minutes.

ACTIVITY SEVEN: PLANNING AN AUDIT

PURPOSE

- To provide you with the opportunity to review and prepare an audit plan for Bangalore Business Solutions.

TASK

- In your team:
  - Prepare an audit plan for Bangalore Business Solutions based on the audit questionnaire, background information pre-audit report, and the results of the analysis of the ISMS Manual.
  - Verify the scope of the ISMS certification to ISO/IEC 27001 ISMS.
  - Decide how you will conduct the audit using available resources (your audit team) based on the information in the questionnaire and pre-audit report.
  - Write a scope for the audit.
  - Identify appropriate areas, individuals and any documents that you wish to see in order to conduct the audit.
  - Produce a detailed audit plan to gain evidence that the ISMS is being implemented effectively, identifying relevant personnel, functions and levels for each of the situations.

OUTPUT

- Be prepared to feedback your findings to the whole group.
- Learner output – Presentation.

TIME ALLOWED

- Activity: 45 minutes.
- Feedback: 45 minutes.

SESSION SEVEN

DEVELOPING THE CHECKLIST

DEVLEOPING THE CHECKLIST

OBJECTIVES

When you have completed this session, you will be able to:

- Explain the use of the “Turtle Diagram”.
- Understand the use, benefits and potential limitations of using checklists.

KEY POINTS

- The audit checklist.
- Process review.
- The “Turtle Diagram”.

DEVELOPING THE CHECKLIST

PROCESS REVIEW

In some situations, there may not be explicit documents such as procedures or work instructions that enable the Auditor to develop a checklist easily. Instead, the Auditor may be faced with little more than a process map covering several complicated task and activities.

Nonetheless, the Auditor will need to ensure that the tasks and activities needed to deliver the process information security objectives and the audit criteria have been addressed.

The Auditor may gain an understanding of the factors involved in a process by:

- Mapping the processes based on the requirements of the relevant standard; or
- Developing a “turtle diagram”.

THE “TURTLE DIAGRAM”

WHEN TO USE A “TURTLE DIAGRAM”

A “Turtle Diagram” may be used in any audit process.

CONSTRUCTING A “TURTLE DIAGRAM”

The “Turtle Diagram” acts as a checklist for organising thoughts and questions around the key principles of any process. It is a “memory jogger”. An example of a “Turtle Diagram” is set out in Appendix 6.

The “Turtle Diagram”:

- acts as a prompt to identify and investigate the various elements of the process – objectives, outputs, results, inputs, what, who and how;
- may be adapted or amended as required. Those elements which are not appropriate may be deleted and any other elements which should, or could, be addressed may be added.

The completed “Turtle Diagram” may be used:

- to compile a checklist; or
- in place of, or in addition to, a separate, detailed checklist.

AUDIT CHECKLIST

The development of the checklist takes place after the Auditor has gained an understanding of the scope, process performance and the sequence of process activities or interaction.

The checklist is a valuable aid to auditing and is used as a working document, and a record.

The compilation of a checklist is a way of analysing the processes involved.

The purpose of a checklist is to ensure that the objectives and scope of the audit are met, and that every part of the audit is completed.

The checklist acts as a guide for the Auditor. It is the Auditor's main tool in carrying out the audit successfully.

ADVANTAGES OF USING A CHECKLIST

The advantages of using a checklist are:

- as an aid in preparing for the audit;
- the number of questions and size of samples can be used to estimate the time required to conduct an audit or parts of an audit;
- an aid to the Auditor to control the depth and pace of the audit;
- an aid to the Auditor to ensure that all of the planned arrangements for the audit are covered; and
- as a means of recording responses by auditees.

DISADVANTAGES OF USING A CHECKLIST

However, there are disadvantages with using a checklist:

- the use of standardised checklists may stifle initiative and analysis of the processes or procedures;
- it may prevent the Auditor from investigating significant incidents simply because they were not on the checklist.

CHECKLIST PREPARATION

In preparing the checklist, the Auditor should consider:

- the processes which are taking place;
- any relevant procedures;
- the documents and records which are being used;
- the requirements of the standard; and
- the requirements of the management system.

The complexity or detail on a checklist will depend on the experience of the Auditor.

An example of a ‘blank’ audit checklist is set out in Appendix 4. An example of a completed audit checklist is shown in Appendix 5.

ACTIVITY EIGHT: AUDIT ROLE-PLAY: PART ONE: PREPARING FOR THE AUDIT

PURPOSE

- To prepare for an audit against the requirements of ISO/IEC 27001:2022.
- It consists of three parts:
  - Part One - is the preparation for the audit (role-play);
  - Part Two - is the conduct of the audit (role-play);
  - Part Three - is the completion of an audit report together with any nonconformities and/ or opportunities for improvement that you have identified, on the forms provided.
- **This activity comprises the role-play** of an audit against the requirements of ISO/IEC 27001:2022.

TASK

- You have been asked to conduct an audit of Bangalore Business Solutions.
- The role-play focuses on a meeting with the top management to audit the organisation's continual improvement processes. You are looking for evidence that there is a planned and systematic approach to continual improvement in accordance with the requirements of ISO/IEC 27001:2022.
- You are looking for evidence that there is a planned and systematic approach to continual improvement in accordance with the requirements of ISO/IEC 27001.
- To conduct the audit effectively:
  - Develop a checklist on the forms provided that addresses at least ten requirements which together cover the following areas
    - the ISMS policy;
    - ISMS objectives and plans;
    - the internal audit programme and management review.

TASK, CONTINUED

- Your preparation should cover the following areas as a minimum:
  - confirmation that the ISMS policy is appropriate to the nature and scale of the organisation's risks;
  - the methods by which the policy is communicated to employees;
  - consideration was given to interested parties and how they are given access to the policy;
  - the reasoning behind the establishment of ISMS objectives and plans;
  - the method by which the policy and plans have been communicated throughout the organisation;
  - the determination of resources to ensure that the ISMS is effective;
  - reports on the performance of the ISMS are produced and the actions taken as a result of these reports;
  - the planned arrangements for the internal audit of the ISMS;
  - the output from the management review is consistent with the organisation's commitment to continual improvement of the ISMS.
- During the role-play, you may:
  - use any documents that you have prepared for this audit (for example, the checklist);
  - speak to top management in the organisation that you are auditing;
  - see any document in the organisation that you are auditing.
- You will be expected to:
  - speak to personnel;
  - listen to responses from auditees and provide feedback;
  - record audit evidence;
  - ensure that confidentiality in respect of proprietary information is applied.

TASK, CONTINUED

- Upon completion of the audit, prepare an audit report together with any nonconformities and/ or opportunities for improvement that you have identified, on the forms provided.
- The tutor will nominate a team leader for the audit role-lay for each team.

PART 1: PREPARATION FOR THE AUDIT

- Decide how you will conduct the audit using available resources.
- Identify appropriate areas, individuals and any documents that you wish to see in order to conduct the audit.
- Carry out a document review on the appropriate and available documents and prepare any work documents that you feel are necessary or appropriate for use during the audit role-play. These should include an audit checklist, sampling plans and any forms that you feel are appropriate.
- Teams can make a “telephone appointment” with the person responsible for the ISMS at Bangalore Business Solutions to clarify any issues not immediately apparent from the information supplied.

TIME ALLOWED

- Activity: 75 minutes
- Feedback: As appropriate

SESSION EIGHT

CONDUCTING THE ON-SITE AUDIT (AUDIT STAGE 2)

CONDUCTING THE ON-SITE AUDIT (AUDIT STAGE 2)

OBJECTIVES

When you have completed this session, you will be able to:

- Explain the process of, and different methods for, gathering evidence during an audit.
- Describe the purpose, structure, content and attendees typically at opening meetings.
- Explain the roles and responsibilities of Guides.
- Describe the benefits and limitation of sampling.
- Understand how to conduct and control audits.
- Gathering audit evidence.
- Appreciate the various techniques of questioning auditees.
- Identify the channels of communication between Auditors and auditees.

KEY POINTS

- Collecting and verifying information.
- Opening meeting.
- Roles and responsibilities of Guides.
- Conducting the audit.
- Questioning techniques.
- Controlling the audit.
- Communication with the audit client and auditee.

CONDUCTING THE ON-SITE AUDIT (AUDT STAGE 2)

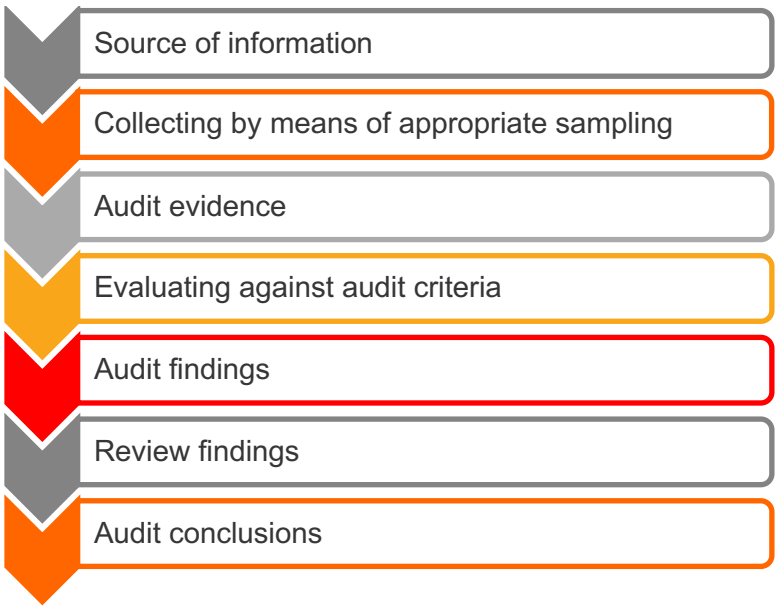
INTRODUCTION

The purpose of the Stage 2 audit is to evaluate the implementation, and effectiveness, of the client's management system. The Stage 2 audit will take place at the site(s) of the client. The areas covered during the Stage 2 audit will include:

- information and evidence about conformity to the requirements of the applicable management system standard or other normative document;
- performance monitoring, measuring, reporting and reviewing against key performance objectives and targets;
- the client's management system and performance in respect of legal compliance;
- operational control of the client's processes;
- internal auditing and management review;
- management responsibility for the client's policies;
- links between the normative requirements, policy, performance objectives and targets, any applicable legal requirements, responsibilities, competence of personnel, operations, procedures, performance data and internal audit findings and conclusions.

This diagram below shows an overview of the audit process of collecting and verifying from ISO 19011.

Collecting and verifying information



COLLECTING AND VERIFYING INFORMATION

ON-SITE AUDIT PROCESS

In a certification audit, the on-site audit is known as Audit Stage 2.

Information collected during the audit should be verified by the Auditors and can then be considered to be “audit evidence”.

AUDIT EVIDENCE

ISO 19011:2018 defines ‘audit evidence’ as:

“Records, statements of fact or other information which are relevant to the audit criteria and verifiable.”

Audit evidence should be identified, documented and recorded. The Auditor will need to obtain information about:

- people;
- processes;
- equipment;
- documentation.

This is done in several ways, such as:

- interviews;
- observations of activities and the surrounding work environment and conditions and infrastructure;
- documents, for example:
  - policy;
  - objectives;
  - plans, and
  - procedures.
- instructions, licences, specifications, recipes, contracts and orders.

AUDIT EVIDENCE, CONTINUED

- records such as:
  - activity logs;
  - inspection and monitoring records;
  - minutes of meetings;
  - reports on customer complaints and other relevant communication from external interested parties;
  - audit reports;
  - monitoring programmes; and
  - results of measurements and reviews.
- data summaries, analyses, metrics and performance indicators;
- records of the basis of relevant sampling programmes and the procedures for ensuring effective quality control of sampling and measurement processes;
- reports from other sources, for example, customer feedback, external reports and vendor supplier ratings;
- computerised databases and websites.
- Information should also be collected relating to interfaces between functions, activities and processes.

The step-by-step process of tracking activities, following leads and ascertaining evidence to obtain information is called an “audit trail”.

The audit evidence collected during an audit will inevitably be only a sample of the information available, since an audit is conducted during a finite period of time and with limited resources.

Therefore there is an element of uncertainty inherent in all audits, and attention of users of the audit conclusions should be drawn to this uncertainty.

SAMPLING

The purpose of sampling

An Auditor cannot interview every person, observe every activity or task, examine every document and record; there simply isn't time to do this.

An audit must be based on sampling enough evidence to be able to establish, with confidence, the degree of conformity demonstrated in the process under review.

The objective of audit sampling is to provide information for the Auditor to have confidence that the audit objectives can or will be achieved.

The risk associated with sampling is that the samples may be not representative of the population from which they are selected, therefore the Auditor's conclusion may be biased and be different to that which would be reached if the whole population was examined.

There may be other risks depending on the variability within the population to be sampled and the method chosen.

Audit sampling typically involves the following steps:

- establishing the objectives of the sampling plan;
- selecting the extent and composition of the population to be sampled;
- selecting a sampling method;
- determining the sample size to be taken;
- conducting the sampling activity;
- compiling, evaluating, reporting and documenting results.

When sampling, consideration should be given to the quality of the available data, as sampling insufficient and inaccurate data will not provide a useful result.

The selection of an appropriate sample should be based on both the sampling method and the type of data required, for example, to infer a particular behaviour pattern or draw inferences across a population.

Reporting on the sample selected could take into account the sample size, selection method and estimates made based on the sample and the confidence level.

Audits can use either judgement-based sampling or, less frequently, statistical sampling.

Judgement-based sampling

Judgement-based sampling relies on the knowledge, skills and experience of the audit team.

For judgement-based sampling, the following can be considered:

- previous audit experience within the audit scope;
- complexity of requirements (including legal requirements) to achieve the objectives of the audit;
- complexity and interaction of the organisation's processes and management system elements;
- degree of change in technology, human factor or management system;
- previously identified key risk areas and areas of improvement;
- output from monitoring of management systems.

A drawback to judgement-based sampling is that there can be no statistical estimate of the effect of uncertainty in the findings of the audit and the conclusions reached.

The objective of auditing is to determine whether the organisation's 'system' is working, in which case large samples are not often required.

Statistical sampling

If the decision is made to use statistical sampling, the sampling plan should be based on the audit objectives and what is known about the characteristics of overall population from which the samples are to be taken.

- Statistical sampling design uses a sample selection process based on probability theory.
- Attribute-based sampling is used when there are only two possible sample outcomes for each sample (for example; correct / incorrect or pass / fail).
- Variable-based sampling is used when the sample outcomes occur in a continuous range.

Statistical sampling, continued

The sampling plan should take into account whether the outcomes being examined are likely to be “attribute-based” or “variable-based”. For example, when evaluating conformance of completed forms to the requirements set out in a procedure, an attribute-based approach could be used. When examining the occurrence of information security incidents or the number of breaches, a variable-based approach would likely be more appropriate.

The key elements that will affect the audit sampling plan are:

- the size of the organisation;
- the number of competent Auditors;
- the frequency of audits during the year;
- the time of individual audit;
- any externally required confidence level.

When a statistical sampling plan is developed, the level of sampling risk that the Auditor is willing to accept is an important consideration. This is often referred to as the acceptable confidence level. For example, a sampling risk of 5% corresponds to an acceptable confidence level of 95%. A sampling risk of 5% means the Auditor is willing to accept the risk that 5 out of 100 (or 1 in 20) of the samples examined will not reflect the actual values that would be seen if the entire population was examined.

When statistical sampling is used, Auditors should appropriately document the work performed. This should include:

- a description of the population that was intended to be sampled;
- the sampling criteria used for the evaluation (e.g. what is an acceptable sample);
- the statistical parameters and methods that were utilised, and the number of samples evaluated and the results obtained.

OPENING MEETING

An opening meeting should be held with the management of the organisation being audited or, where appropriate, those responsible for the functions or processes to be audited. Records of attendance at the opening meeting should be kept.

OPENING MEETING, CONTINUED

The purpose of the meeting is to:

- present or to confirm the audit plan;
- clarify how the audit activities will be undertaken;
- establish communication.

The meeting should be chaired by the audit team leader and the following items considered, as appropriate:

- introduction of the participants, including an outline of their roles;
- confirmation of the audit objectives, scope and criteria;
- confirmation of the audit plan and other relevant arrangements with the auditee, such as the date and time of the closing meeting, any interim meetings between the audit team and the auditee's management, and any late changes;
- methods and procedures to be used to conduct the audit, advising the auditee that the audit will only be a sample of the information available and of the element of uncertainty inherent in all audits;
- confirmation of formal communication links between the audit team and the auditee;
- confirmation that during the audit, the auditee will be kept informed of audit progress;
- confirmation that any equipment, other resources and facilities needed by the audit team are available;
- confirmation of matters relating to confidentiality;
- confirmation of relevant work safety, emergency and security procedures for the audit team;
- confirmation of availability, roles and identity of any Guides;
- method of reporting including the classification of non-conformities;
- information about any audit appeal system.

At the end of the opening meeting, opportunity should be given to the auditee to ask any questions.

An example checklist for an opening meeting is set out in Appendix 7.

OPENING MEETING, CONTINUED

In many audit situations; for example: “surveillance audits” or “internal audits”, the opening meeting may consist of simply that an audit is taking place, so the above list is neither prescriptive nor exhaustive.

The golden rules are:

- keeping it brief and concise; and
- keeping control.

Following the opening meeting, Auditors may request a short tour of the premises to familiarise themselves with the layout of the organisation.

Opening meetings for internal audits may be less formal. Guides, representatives, formal opening and closing meetings may not be necessary for internal audits.

ROLES AND RESPONSIBILITIES OF GUIDES

Where Guides are assigned, they should assist the audit team and act on request of the audit Team Leader. Their duties may include ensuring that rules concerning safety and security (access) procedures are known and respected by the Auditors on-site. They may also witness the audit on behalf of the auditee.

Guides should not exercise undue influence or interference, except where, with the agreement of the Auditor, the Guide can provide clarification or assist in establishing correct information.

CONDUCTING THE AUDIT

AUDITING – THE PEOPLE ISSUES

Effective auditing involves:

- Good planning; and
- Preparation.

AUDITING – THE PEOPLE ISSUES, CONTINUED

What are the risks from interpersonal element of an audit?

- The auditee does not cooperate for whatever reason.
- The auditee genuinely feels that the process was not fair.
- There is just cause for complaint about the Auditor's behaviour.
- The Auditor does not effectively find out the status of the process under audit.

Audits always involve interviews and, are therefore, a person-to-person experience for both parties. The auditee may feel:

- Picked-upon;
- Apprehensive;
- Nervous;
- Threatened;
- Angry; and
- Keen to unburden themselves.

Be that as it may, the Auditor needs to be:

- Alert and relaxed - quickly picking up the auditee's condition/attitude;
- Friendly and polite;
- Non-threatening;
- Attentive to the auditees needs and attitude;
- Capable of being gently persistent;
- Able to realise when the auditee is puzzled by the question being asked;
- Able to listen.

AUDITING – THE PEOPLE ISSUES, CONTINUED

The whole process depends on the Auditor. The auditee did not ask the Auditor to be there so the Auditor must manage the whole situation to ensure that:

- All of the ground that was planned to be covered is covered;
- Any changes are coped with;
- Situations are controlled without being aggressive;
- The auditee is comfortable, relaxed and communicative;
- No-one has just cause to consider a complaint;
- The process is seen to be of value;
- The agreed timescales are kept to.

The human interaction is very important, especially the first impression. The Auditor needs to think about:

- Dress - in keeping with the audit;
- The introductions;
- The smile of greeting;
- The language that they use;
- Small talk.
- Where and how the audit is being carried out, for example:
  - Should the Auditor stand or sit?
  - How should the checklist be used?
  - The number of people surrounding the auditee.

The Auditor should treat the auditee as they would like to be treated.

Body language is important and the Auditor should trust his or her intuition and should be aware of their own body language:

- If people appear nervous – they are!
- If they appear upset – they are!
- If they appear evasive – they are!

AUDITING – THE PEOPLE ISSUES, CONTINUED

The Auditor should try to understand why they feel that way, for example:

- Did they not understand the question?
- Is there something to hide?
- Are they uncomfortable with this inquisition?
- Do they disagree with the findings, but will not say so?
- Is there some other reason - from their home life perhaps?
- Is the Auditor being sensitive to their needs?

In these circumstances the Auditor should:

- Quickly appraise the situation and, if necessary defuse it.
- Take a break.
- Enquire about the 'problem'.
- Have they misunderstood?
- Is the Auditor being too pedantic?

The right outcome is that the:

- Auditee feels that the process was fair and not upset by your attitude.
- Process was effectively audited.
- Conclusions drawn were fair, accurate and accepted.

POSITIVE AND PROFESSIONAL

The Auditor should adopt a positive, professional and constructive approach. In common with this, the Auditor should try to obtain a co-operative, open and honest approach from the auditee.

POSITIVE AND PROFESSIONAL, CONTINUED

To achieve these objectives, the Auditor should:

- Meet the area representative first.
- Always talk to those performing the task.
- Explain the purpose of the visit.
- Be calm, polite and reassuring.
- Never talk down, never act superior.
- Speak clearly and carefully.

Interviews are an important means of collecting information and should be carried out in a manner adapted to the situation and person interviewed. However, the Auditor should consider the following:

- Interviews with persons from different levels and function, and especially with persons performing activities or tasks under consideration.
- Whenever possible, the interview should be conducted during normal working hours and at the normal workplace of the interviewed person.
- Every attempt should be made to put the interviewed person at ease prior to the interview,
- The reason for the interview and any note taking should be explained.
- Interviews may be initiated by asking the persons to describe their work.
- The results from the interview should be summarised and any finding should be verified with the interviewed person where possible.
- Leading questions should be avoided.
- The interviewed persons should be thanked for their participation and co-operation.

QUESTIONING TECHNIQUES

CLOSED QUESTIONS

Closed questions (which receive a ‘yes’ or ‘no’ answer) are used to elicit information in small packages and invite a brief response from the interviewee.

CLOSED QUESTIONS, CONTINUED

For Auditors, the best use of the closed question is to confirm factual details.

- “Are you the only person doing this yob?”
- “Is that where you keep the records?”
- “Have you had any training for this?"

An interview that proceeds along these lines is more like an interrogation than a conversation, and the information is strictly factual, with no explanations or clarifications.

Auditors interview in order to gather information as to whether a process is working effectively, “closed” questions do not always achieve this.

A good audit will comprise 70% open questions, 30% closed; 60:40 is not bad, but anything that tips the balance towards more closed questions will mean that the audit is very stilted and a difficult situation for both the Auditor and auditee.

OPEN QUESTIONS

There are six words that are important to any Auditor. These are:

- How?
- Where?
- What?
- Why?
- Who?

You should ask efficient, open-ended questions to elicit information and avoid terse, monosyllabic replies. Open-ended questions invite the interviewee to “open-up” on a topic.

They encourage the interviewee to speak, rather than nodding their response. For example:

- “How are you getting on?"
- “What records do you complete?"
- “Where do you keep the documents?"
- “How were you trained for this?”

OPEN QUESTIONS, CONTINUED

This style of questioning makes it easier for the interviewee. They are being given the space to speak and to relax. They begin to talk, hear themselves talk and develop their poise. The interview becomes more of a conversation, than a hard-nosed audit.

However, you will need to continue to focus on the task under question in order to maintain the control and direction of the audit.

There is another key phrase the Auditor should use regularly:

- “Show me.”

FOLLOW-UP QUESTIONS

These questions are used to develop and focus an answer to an open-ended question:

- “What about the documents you use?"
- “Where did you say you keep the file?"
- “Is that right, you received only on-the-job training for this?"

SUMMARY AND RE-RUN

This is the process of drawing together, in summary, various points from the interviewee and obtaining their confirmation.

As the interview progresses, the interviewee will produce lots of information. You will need to select that which is important to retain and understand.

Periodically, you may interject a summary sentence with an interrogative inflection:

- “So, the way this is described in the procedures is not accurate?"
- “So, this part of the document is not completed because they do not give you the exact information?"

You need to ensure that you keep control of the interview and focussed on the issues that you need information for.

And of course, at the end of the interview, make sure that you thank the interviewee for their co-operation and openness.

CONTROLLING THE AUDIT

The Auditor must control the audit.

- Do not:
  - be side-tracked;
  - be led or misled;
  - let the auditee dictate the pace of the audit;
  - make assumptions or presumptions.
- Do:
  - be prepared;
  - be punctual;
  - insist on the person be questioned being able to answer for themselves;
  - as little talking as possible;
  - avoid misunderstandings;
  - keep questions clear and concise;
  - be polite and calm;
  - give compliments.

The Auditor must be prepared for, and be aware of, a range of possible occurrences during the course of the audit. For example:

- aggressive auditees;
- timid auditees;
- missing people;
- missing documents;
- pre-prepared samples (always choose your own);
- special cases;
- local issues and cultural customs;
- emotional blackmail.

CONTROLLING THE AUDIT, CONTINUED

When faced with these situations, the Auditor must act decisively, professionally and fairly, keeping in mind the objectives and purpose of the on-site audit.

COMMUNICATION DURING THE AUDIT

Depending on the scope and complexity of the audit, it may be necessary to establish formal arrangements for communication during the audit.

An audit team should confer periodically in order to exchange information, assess audit progress and reassign work between Auditors as needed.

During the audit, the Team Leader should periodically communicate the status of the audit and any concerns to the auditee and audit client, as appropriate.

Where the available evidence indicates that the audit objectives are unattainable, the audit Team Leader should report the reasons to the audit client and the auditee to determine the appropriate action, which may include termination of the audit or a change in the audit objectives.

Any concern about an issue outside the audit scope should be noted and reported to the audit team leader, for possible communication to the audit client and auditee.

Any need for changes in the audit scope which may become apparent as on-site auditing activities progress should be reviewed with and approved by the audit client and, as appropriate, the auditee.

SESSION NINE

AUDIT REVIEW

AUDIT REVIEW

OBJECTIVES

When you have completed this session, you will be able to:

- Describe the purpose, structure, content and attendees typically at audit review meetings.
- Understand the processes of identifying and drafting finding statements.
- Explain the methods for identifying nonconformities.
- Describe the purpose and typical content of Corrective Action Request (CARs).
- Describe the classification of CARs and the implications.
- Describe the use of “opportunities for improvement”.
- Explain further actions required for the different grades of CARs.

KEY POINTS

- Audit review meeting.
- Audit findings.
- Finding statements.
- Corrective Actions Requests (CARs).
- Classification of CARs.
- Opportunities for improvement.

AUDIT REVIEW

AUDIT REVIEW MEETING

When the audit is complete, the Auditor team leader must conduct a private review of the findings with the members of the audit team. Interim or end of day reviews may also be necessary. The review will involve all the members of the audit team.

The review will include:

- a study of notes and/or comparison of notes with team members;
- a review of checklists;
- the listing of findings, together with any audit evidence;
- decisions on nonconformities and opportunities for improvement;
- the writing and classification of Corrective Action Requests (CARs).

AUDIT FINDINGS

Until it is classified, an audit finding may be a:

- Non-conformity;
- Opportunity for improvement or “observation”.

A nonconformity arises when the process or procedure being audited is not being conducted or completed as it should. A nonconformity is defined as:

- The non-fulfilment of a requirement.

Therefore, a nonconformity may be a failure to:

- comply with the standard applicable to the organisation;
- implement information security policy, process or documented requirements specified by the organisation;
- Implement a legislative or contractual requirement.

If there is no specified requirement, there can be no nonconformity. What an Auditor thinks should be done is not a specified requirement.

AUDIT FINDINGS

Nonconformities should be recorded and supported by audit evidence. Nonconformities should be reviewed with an appropriate auditee representative to obtain acknowledgement of the audit evidence.

The auditee representative's acknowledgement indicates that the audit evidence is accurate, and that the nonconformity is understood. Every attempt should be made to resolve any divergence of opinion concerning the audit evidence, and unresolved points should be recorded.

Sometimes during an audit, an Auditor may identify a minor deficiency that is then effectively resolved by management before the closing meeting. In a situation such as this, provided the Auditor is convinced that the matter has indeed been resolved and it is not symptomatic of a common problem throughout the organisation, it need not be raised formally at the closing meeting. A record should be made by the Auditor to verify that the action implemented is complete and acceptable.

WHEN ARE FINDING STATEMENTS WRITTEN?

A "finding statement" is a description of the conformity or nonconformity discovered during the audit.

Some auditing organisations insist on finding statements being written out immediately a deficiency is identified and the representative's signature obtained. However, an Auditor should ensure that all relevant evidence is gathered before making a decision.

The best practice is to go over the facts verbally and agree the nature of the nonconformity with the auditee, detailing the audit evidence:

- make notes and consult these later to make a statement;
- draft finding statements during a working lunch or at the end of the day, then finalise at the private review.

When working as a member of an audit team, the Auditor will need to review the evidence with the team leader before deciding the wording of a finding statement and its classification.

FINDING STATEMENT

The finding statement should contain:

- a clear statement of the nonconformity;
- the (detailed) objective evidence on which the nonconformity is based;
- summary of the requirement.

Below are examples of finding statements:

GOOD EXAMPLES

- ‘Good’ Example One:

  The background screening process during recruitment process is not effective.

  Organization’s CFO background check indicated that he/she served 5 years in prison for embezzlement.

  - Background verification checks on all candidates to become personnel shall be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

- ‘Good’ Example Two:

  The background screening process during the recruitment process is not effective.

  For 5 new employees (all starting between January and May 2022), no evidence of background verification checks were available.

  - Background verification checks on all candidates to become personnel shall be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

FINDING STATEMENT, CONTINUED

- ‘Good’ Example Three:

  Back-up process not effective.

  Organisation’s payroll system server had a dual hard disk failure. A back-up was not made since January 2020.

  - Back-up copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on back-up.

BAD EXAMPLES

- ‘Bad’ Example One:

  Organisation’s process for segregation of networks is non-conforming.

  Groups of information services, users and information systems shall be segregated in the organisation’s networks.

  - Why ‘Bad’? - The description of what was not segregated was missing.

- ‘Bad’ Example Two:

  The organisation failed to protect personal indefinable information as per GDPR requirements.

  - Why ‘Bad’? - What are the requirements of GDPR that are violated, and more importantly this audit is at a company in Singapore --- why would GDPR be applicable?

- ‘Bad’ Example Three:

  Management review meetings not completed as required and meeting minutes don’t address all requirements of ISO/IEC 27001.

  - Why ‘Bad’? - (1) There is no requirement for a meeting and (2) What exactly is missing?

BAD EXAMPLES, CONTINUED

- 'Bad' Example Four:

  The organisation does not maintain a membership or contact with (ISC)2.

  - Why 'Bad'? - So, what? What is the violate requirement (missing Annex A 5.6). Do they maintain contact with any other special interest groups or other specialist security forums and professional associations?
  - Number of similar nonconformities may be grouped by process, function, procedure or standard clause into a single finding statement.

CORRECTIVE ACTION REQUEST (CAR)

This is a form used by many organisations (see Appendix 8). It is used to describe a nonconformity or noncompliance and request action. It may also be known as a nonconformity report, noncompliance notice, etc.

The CAR is raised after careful consideration at the audit review prior to the closing meeting with the organisation.

The CAR form is used to:

- report nonconformities;
- show the level or classification of those nonconformities;
- record acceptance of the nonconformity by the auditee (usually the audited organisation's representative);
- record the actions taken to correct the nonconformity;
- record acceptance by the Auditor of the corrective action taken to resolve the nonconformity.

The CAR should contain references to:

- the applicable process, function or procedure;
- Standard and clause number;
- location and date;
- Auditor's name;
- finding statement.

CLASSIFICATION OF NONCONFORMITIES

The classification given to a nonconformity can vary from one organisation to another but the following is typical:

Major nonconformity

A Major nonconformity is raised where there is a:

- failure to fulfil one or more requirements of the standard; or
- situation that raises significant doubt about the ability of the ISMS to achieve its intended outputs.

In general terms this would be where the nonconformity is likely to result in an immediate risk to the information security, such as:

- the absence of, or substantial failure to meet the requirements of the standard; or
- when the nonconformance(s) indicate a total breakdown of a process or procedure significant to information security, or in the effective operation of the misuse of a certification mark or an accreditation mark which misrepresents their certification.

Minor nonconformity

Raised when a deficiency (or deficiencies) have been identified in a process in the operation of the organisation's management system, but which are less severe than warrants a major CAR.

The classification of CARs is based upon good judgement, expertise and experience of the Auditor, and may have far-reaching consequences.

CONSEQUENCES OF RAISING NONCONFORMITIES

If a major nonconformity (NC) is raised during an initial third-party audit, the nonconformity must be corrected and the corrective action to prevent recurrence must be verified before certification can be recommended.

If raised during a surveillance audit, the Major NC, if not corrected, may lead to certification being withdrawn.

CONSEQUENCES OF RAISING NONCONFORMITIES, CONTINUED

A Minor NC allows certification to proceed. The corrective action taken is usually verified at the following surveillance visit.

If not closed, a Minor NC will be re-classified as a Major.

In second-party audits, a major NC may result in contracts being withdrawn, not awarded or renewed.

Minor NCs are usually corrected and verified as agreed between the two organisations,

The classification of nonconformities is not necessary for internal audits. CARs are meant to assist management in improving the system and in internal auditing, and may be supported by recommendations to correct and improve the ISMS. Audits, therefore, should be positive and constructive. Effective corrective action is more important.

OPPORTUNITY FOR IMPROVEMENT

Audit findings may also take the form of “Opportunities for Improvement”, “Observations” or “Comments”.

In many ways, “Opportunities for Improvement” are the added-value part of the audit. They are the points on which the Auditor may wish to comment but for one reason or another, are not reported as CARs.

Opportunities for improvement may include:

- good practices which could benefit other processes within the organisation;
- areas of concern which are not yet serious enough to warrant CARs;
- situations which if not addressed may give rise to CARs at a later date;
- deficiencies for which the Auditor is prepared to give the organisation the “benefit of the doubt”, and
- suggestions for action to improve the effectiveness of the management system.

Opportunities for improvement provide a flexible method of reporting for the Auditor in that although they have no formal status, opportunities for improvement can make the difference between a positive and negative audit.

OPPORTUNITY FOR IMPROVEMENT, CONTINUED

Because opportunities for improvement can add value to an audit, many organisations regard them in much the same way as CARs; that is, actions taken in response to opportunities for improvement are reviewed and evaluated during future audits.

AUDIT CONCLUSION

Having reviewed and analysed all of the information and audit evidence gathered during the Stage 1 and Stage 2 audits, the audit team will agree on the audit conclusion to be presented to the management of the organisation that has been audited.

ACTIVITY NINE: INTERPRETATION OF THE STANDARD

PURPOSE

- To identify and classify nonconformities in respect of ISO/IEC 27001:2022 and record findings statements.
- Note: There are two parts to this Activity.

TASK: PART ONE

- The incidents below occur during a third-party audit. In each of the situations, there may be nonconformity in respect of ISO/IEC 27001:2022 requiring a CAR to be raised. Examine each incident and take the following actions:
- In the event that you decide a situation provides evidence of nonconformity, classify the nonconformity as Major or Minor.
- Determine the number of the clause from ISO/IEC 27001 that identifies the nonconformity.
- Select any two of the nonconformities and write out finding statements that would be presented to management on the CAR forms provided.
- In the event that you decide a situation provides insufficient evidence of nonconformity, state why you think there is insufficient evidence and make a list of things you would look for as evidence that the situation is under control.

EXAMPLE

A team of Auditors assessing an organisation on a two-day audit determine that there is a general lack of understanding of the information security policy by personnel in the following departments: Purchasing, Sales/Contracts, Design and manufacturing.

Clause: 7.3 Awareness

TASK: PART TWO

- You will be given a number of CARs that have been raised during some recent audits.
- Evaluate proposals for corrective action and differentiate between correction and corrective action.
- Record your acceptance and/or comments of the proposed corrective action in the space provided on the form.
- Be prepared to discuss your findings with the course tutor.

OUTPUT

- Be prepared to feedback your findings to the whole group.
- Learner output – Presentation.

TIME ALLOWED

- Activity: 180 minutes.
- Feedback: 45 minutes.

1)	During the document review, the Auditor noted that Security Procedure SP04 required that suitable background checks be undertaken on all employees. At the company, the Auditor found that checks had not been carried out on the receptionist, the security guards and one of the system administrators, who is a relative of the Chief Executive.
	Clause: Classification:
2)	In an unused office, the Auditor noticed a computer (S/N GZF-0B-45678). The guide said that this office had been used by Mrs Chang who had left the company unexpectedly three weeks ago. The computer contained a 40GB hard drive. The audit asked whether the computer had been re-formatted to remove any sensitive material. The ISMS Officer told the Auditor that the computer would be passed to the person who would replace Mrs Chang and any unnecessary information would be removed at that time. This was not unusual as it saved time.
	Clause: Classification:

3)	During a routine surveillance visit, the Security Manager tells you that the organisation no longer carries out any design work. This activity is now outsourced to a sub-contractor. This sub-contract company has been set up by a previous manager of the organisation and so there is an understanding of the systems that the audited organisation operates and the security risks and treatments involved in their ISMS. There is no need to carry out a full risk assessment on this aspect of outsourced processes, beside which, you are told, the sub-contractor is in the process of implementing an ISM based on ISO/IEC 27001.
	Clause: Classification:
4)	In an area dedicated to disposal of failed and redundant IT equipment, the Auditor examines the disposal record for asset number 1234, a laptop PC. The Auditor notes that in the final inspection records, the word 'OK' is written next to the statement that all information has been securely erased from the device. The record shows that this laptop PC has been bought from the company by an employee for their private use. When asked about this, the Manager explains that usable equipment is sold internally with proceeds going to a nominated charity. The Auditor asks that the laptop booted up and it shows a Microsoft Windows XP® operating system. Further inspection of File Explorer indicates that the file system is apparently empty.
	Clause: Classification:

5)	In an Insurance Broker (ABC Compare.com), while reviewing the system archive, the Auditor came across several security events had been found by the IDP system, an internet intruder detect system. These had been entered into the Computer Operator Log over the past two months for 11 employees all of whom were attempting to connect to MSN via an external proxy server. As this is against corporate policy, individual members of staff had been advised that this practice was to cease but it seemed to be continuing especially on the night shifts.
	Clause: Classification:
6)	The audit is being conducted on XZY Solutions, an organisation that provides collects, integrates and collates patient data from a private hospital facility (Beds-R-US). The Auditor notes that attached to the latest issue of the contract is an amendment that includes a requirement that all patient data is held in accordance with the Hospital Procedures BRU 341. The Contracts Manager informs the Auditor that he is not aware of this requirement and is not familiar with Hospital Procedure BRU 341. The Auditor notes that this amendment was issued 6 months previously; the contract has been in place for 4 years and there is no reference to the Procure BRU 341 in the original contract. The Auditor confirms that patient data is held in accordance with XYZ's own procedures.
	Clause: Classification:

7)	When looking through the logs of the Archserve back-up system, the Auditor noticed that an entry 3 months ago showed that there was a shortage of storage space. The hard disk capacity of file server No. SB0123004 is 240GB currently, but the capacity of the two tape drives are 36GB and 72GB.
	Clause: Classification:
8)	During the third-party audit of the IT Department, the Department Manager demonstrates the capacity management process. The process requires the staff to monitor the capacity, analyse utilization trends and identify the capacity requirements and to develop Capacity Plan for projected capacity requirements. The Auditor inquires that how the utilization trends of different machines / servers, are being monitored and analysed, the Manager replied that a tool is being used which collects the data from all the servers. The Auditor finds that two servers UTL-2345 (Mail server) & UTL-6798 (Domain controller) were not connected to the tool and told these are monitored manually by the IT staff. The Auditor finds that in their actual work, utilization trends not found analysed for these servers and further the capacity plan not implemented for a hard drive of a Server UTL-2345, having 90% capacity utilization whereas the capacity plan of 2014, required it to be upgraded, but it is not done even in the last 6 months (Jun-2014). It was further found by the Auditor that two incidents (Inc. #1113 and Inc. #9972) were reported and related to this server due to lack of space. On inquiry the Manager responded that due to workload and time shortage, the staff is busy identifying and serving the calls received at the service desk / there remains no time to regularly review the utilization of certain machines and to do upgrades.
	Clause: Classification:

9) An ISMS Auditor is reviewing the arrangements for establishing the relevant regulatory requirements and for keeping this up-to-date in an international distributer of manufactured radio communication systems for emergency services. The systems include 'smart' programmed handsets with built-in encryption supporting secure communication services.

The Head of Security who is nominated as the ISMS management representative explains that as she is not a legal expert she has a contract with an external consultant who notifies her by email when any new legislation or regulations is published in the countries to which they export the systems.

There is a dedicated file on the server and it can be seen that developments in key pieces of computer and information legislation have indeed been issued promptly over the previous three years covering the topics expected. The individual notes from the consultant state the title, date and unique reference for the regulation/legislation concerned, along with a summary of what each contains. The Head of Security adds each new item to a rolling two column list entitled "IS International Legislation" which is issue controlled.

The Auditor asks the Head of Security how on-going compliance is monitored. She replies that the consultant visits the organisation once per year and checks that the list entitled "IS International Legislation" does in fact include all the items he has notified to them over the previous year and signs a hard copy of the register after the last entry. On this basis the Head of Security prepares a signed statement for inclusion in the minutes of the annual management review to state "Following periodic review, the organisation remains in compliance with all relevant information security legislation".

Clause:

Classification:

10)	During an audit of the ISMS it is clear that some aspects have not been maintained as you would expect; or indeed in accordance with planned events, including the schedule of internal audits and the closing out corrective actions from previous nonconformities identified within the ISMS. The Management Representative in the organisation is also responsible for the Quality, Environment and OH&S management systems and he informs the Auditor that his deputy resigned eight months previously and has not yet been replaced, and he is unable to maintain all aspects of the ISMS on his own. You confirm from the audit evidence the connection between the deputy resigning and the failure to maintain these aspects of the ISMS.
	Clause: Classification:

SESSION TEN

AUDIT REPORTING AND FOLLOW-UP (STAGE 2)

AUDIT REPORTING AND FOLLOW-UP (STAGE 2)

OBJECTIVES

When you have completed this session, you will be able to:

- Describe the purpose, structure, content and attendees typically at closing meetings.
- Describe the preparation, approval and distribution of audit reports.
- Be aware of the information needed to recommend the certification decision in a third-party audit.
- Understand the role of Auditors and explain the roles and responsibilities for taking and verifying corrective action.
- Explain the steps necessary to address corrective actions.
- Identify the types of evidence that may be required to demonstrate effective implementation of corrective and preventive action.
- Understand the role of the management review.
- Appreciate the steps necessary to follow-up and close out corrective actions.

KEY POINTS

- Presenting the findings.
- Reporting on the audit.
- Audit completion.
- Corrective action.
- CAR status log.
- Management review.
- Follow-up and close out

AUDIT REPORTING AND FOLLOW-UP (STAGE 2)

ADDRESSING CORRECTIVE ACTIONS

PRESENTING THE FINDINGS

When the review and analysis of information and evidence has been completed and a conclusion reached, the Auditor/ team will present the findings to management at a “closing meeting”.

CLOSING MEETING

A closing meeting, chaired by the audit team leader, should be held with the auditee's management and those responsible for the functions audited. Records of attendance at the closing meeting should be kept.

The purpose of this meeting is to present audit findings and conclusions in such a manner as to ensure that they are understood and acknowledged by the auditee and to agree the time period for the auditee to present any corrective action plan.

For internal audits, this may be an informal process. The meeting should be constructive and aimed at system improvement, especially as the Auditor and auditee work for the same organisation and have the same objectives.

For a second-party closing meeting much more care is needed as there are contracts at stake and reports can be used as a future reference. It is a sensitive situation and the Auditor must be prepared to be cross-examined by the auditee on his or her findings.

A third-party closing meeting is usually very formal. The Auditor must be aware that the organisation is the client and as such will expect a comprehensive, detailed and constructive presentation of findings.

Conducting a closing meeting

A closing meeting agenda will vary according to the type of audit conducted, but the following list, which is neither exhaustive nor prescriptive, contains typical items on a closing meeting agenda:

Conducting a closing meeting, continued

- distribute attendance list;
- restate purpose and scope, including any exclusion;
- state decision and conclusion;
- summary of good points within the ISMS;
- explain Major and Minor CARs (asking the client to defer questions);
- explain CAR form completion obtain client representative's signature on CAR;
- explain significance of sampling technique;
- report on opportunities for improvement;
- stress confidentiality;
- explain reporting and follow-up;
- give the client the opportunity to query findings or any other issues;
- have Auditor log signed;
- obtain attendance list;
- thank the client;
- congratulate where appropriate.

During the closing meeting, the Auditor/team leader must:

- thank the client for their hospitality and co-operation;
- explain all findings and evidence carefully and precisely;
- be prepared to support and justify findings;
- avoid being drawn into an argument;
- apologise if an error transpires and alter or withdraw the CAR if necessary;
- refuse the 'quick fix' as a sole solution to the finding. The management must investigate and attempt to correct the root cause of the problem to prevent any recurrence;

REPORTING ON THE AUDIT

AUDIT REPORT PREPARATION AND CONTENT

The audit team leader is responsible for the preparation, accuracy and completeness of the audit report. The audit report should provide an accurate record of the audit and should contain audit conclusions on issues such as the following, if within the audit objectives and scope:

- extent of conformance of the management system to the audit criteria;
- the effective implementation of the management system;
- the ability of the management review process to ensure the continuing suitability and effectiveness of the management system.

The audit report should also include, or make reference to the:

- identification of the organisation or processes audited;
- identification of the audit client;
- agreed audit objectives, scope, exclusions and plan;
- audit criteria, including a list of reference documents, against which the audit was conducted;
- identification of audit team members;
- date(s) and place(s) the audit was conducted;
- audit findings.

The audit report may also include:

- the duration of the audit;
- the identification of the auditee's key representatives and any Guides participating in the audit;
- a summary of the audit process including any obstacles encountered;
- a statement of the confidential nature of the contents;
- a distribution list for the audit report;
- confirmation that the audit objectives have been accomplished within the audit scope in accordance with the audit plan;
- any agreed follow-up action plans;

AUDIT REPORT PREPARATION AND CONTENT, CONTINUED

The audit report may also include (continued):

- any unresolved diverging opinions between the audit team and the auditee; and
- recommendations for improvement.

REPORT APPROVAL AND DISTRIBUTION

The audit report should be issued within the agreed time period. If this is not possible, the reasons for the delay should be communicated to the audit client and a revised issue date should be agreed.

The audit report should be dated and signed by the audit team leader and reviewed and approved as defined in appropriate documented procedures.

The audit report should then be distributed to recipients designated by the audit client.

The audit report is the property of the audit client and confidentiality should be respected and appropriately safeguarded by the audit team members and all report recipients.

An example of an Internal Audit Report Pro-forma is provided in Appendix 9.

An example of a completed Third-party Certification Audit Summary Report is provided in Appendix 10.

RETENTION OF DOCUMENTS

Work documents and reports pertaining to the audit should be retained or destroyed by agreement between the participating parties and in accordance with audit procedures and any applicable requirements.

Unless required to do so by law, the audit team and audit programme management should not disclose the contents of documents, the nature of any other information obtained during the audit, or the audit report, to any other party without the explicit approval of the audit client and, where appropriate, the approval of the auditee.

.

AUDIT COMPLETION

INFORMATION FOR GRANTING INITIAL CERTIFICATION

At the conclusion of the audit, the Auditor or audit team will make a recommendation to the certification body for the decision on certification to be made. That decision will be made on the basis of:

- the audit reports;
- comments on the nonconformities and, where applicable, the correction and corrective actions taken by the client;
- confirmation of the information provided to the certification body used in the application review;
- any conditions or observations.

ADDRESSING CORRECTIVE ACTION

CORRECTIVE ACTION DEFINED

ISO/IEC 27000:2018 defines corrective action as:

"Action to eliminate the cause of a nonconformity and to prevent recurrence."

In processing CARs, the Auditor and auditee have specific responsibilities. The auditee's management must, in conjunction with the management representative:

- investigate and clearly identify the problem;
- propose a programme of long-term corrective action;
- agree a target date for completion;
- introduce changes;
- verify effectiveness by internal audit;
- notify Auditor of conformance;
- link with continuous improvement measures.

CORRECTIVE ACTION DEFINED, CONTINUED

At this stage, one of the responsibilities of the Auditor is to evaluate the proposals for corrective action to ensure the immediate remedial action is taken and that long-term corrective action proposed will prevent a recurrence of the nonconformity.

RESOLVING THE NONCONFORMITY

To resolve the nonconformity, the management of the area that has been audited will:

- take immediate action to correct the nonconformity;
- analyse the effects of the nonconformity on the product or service;
- identify the root cause of the problem;
- initiate a similar investigation into other areas where the problem may exist;
- develop effective actions to prevent a recurrence of the nonconformity;
- implement and monitor the corrective action.

The management representative should:

- approve the proposed corrective actions;
- monitor progress in completing the corrective actions;
- arrange a follow-up internal audit to verify effectiveness.

In third-party audits, the Management Representative is asked to propose a programme of long-term corrective action.

These should be sent to the Auditor. The Auditor should review the new or revised documentation and, as far as possible, evaluate the likely effectiveness of the proposal and discuss this with the auditee if necessary.

FOLLOW-UP AND CLOSE-OUT

AUDIT FOLLOW-UP

The audit client or auditee is responsible for determining any corrective action needed to deal with a nonconformity. Corrective action and subsequent follow-up actions, which may include additional audits, should be completed within an agreed time period. The auditee should keep the Auditor informed of the status of corrective action activities.

Corrective action should be verified in accordance with the appropriate documented procedure. A follow-up report may be prepared and distributed in a manner similar to the original audit report.

The process of determining whether the corrective action requested has been implemented is called "follow-up". This can be completed by reviewing documentation submitted by the client or by visiting the client's premises.

AUDIT CLOSE-OUT

The action relating to the verification and acceptance of corrective action by the Auditor is called "close-out".

Methods of "close-out" will include re-audit of areas in which nonconformities have been identified, where physical evidence has to be seen, or review of new and / or revised documentation.

The Auditor will verify the effectiveness of corrective actions by visiting the organisation and by:

- carrying out an audit of objective evidence;
- verifying that the corrective actions have been implemented;
- ensuring short and long-term effectiveness;
- recording details of the follow-up;
- signing-off the forms.

MANAGEMENT REVIEW

The results on internal and external audits should be reported to the management review.

Here the results will be analysed and the status of corrective actions reported.

Further actions to prevent recurrence impacting on the wider business policy, customer satisfaction, continuous improvement programmes and measures should be identified and implemented if necessary.

ACTIVITY TEN: DEMONSTRATING A CLOSING MEETING

PURPOSE

- To provide you with an example of a formal closing meeting.
- To illustrate good practice at meetings.
- To enable you to participate in a closing meeting.

TASK: PART ONE

- In your team, assume the role of “management” to receive findings.
- The Tutor will:
  - Raise corrective action requests (CARs).
  - Demonstrate the use of attendance lists and Auditor logs.
  - Demonstrate control over the meeting, and
  - Provide answers to questions put by learners as part of the “role-play”
- You should develop your own fictitious organisation and materials (CARs, OFIs, attendance logs, etc.) in keeping with the objectives and spirit of the role-play.

OUTPUT

- Be prepared to feedback your findings to the whole group.

TIME ALLOWED

- Activity: 15 minutes.

ACTIVITY ELEVEN: CASE STUDY

PURPOSE

- To prepare a meaningful and accurate summary of the audit in the form of a formal “closing meeting” to management based upon the analysis of the assigned case study.
- The actions carried out in this activity will constitute the basis of the formal team presentation on the final day of the course.

TASK

- In your team:
  - Read the assigned case-study.
  - Write and agree the audit scope with the management of the organisation concerned.
  - Identify any nonconformities against ISO/IEC 27001.
  - Write and classify the relevant finding statements and Corrective Action Requests (CARs).
  - Prepare a meaningful and accurate summary of the audit in the form of a formal 'closing meeting' to management based upon your analysis of the assigned case-study:
    - recognising and reporting positive findings and opportunities for improvement;
    - making a recommendation (or otherwise) for certification of the organisation based upon audit findings.

OUTPUT

- Be prepared to feedback your findings to the whole group.

TIME ALLOWED

- Activity: 60 minutes (supervised).
- Feedback: 30 minutes (each team).

ACTIVITY EIGHT: AUDIT ROLE-PLAY: PART TWO: CONDUCTING THE AUDIT

PURPOSE

- To conduct a role play of an audit against the requirements of ISO/IEC 27001:2022 and complete an audit report together with any nonconformities and/or opportunities for improvement.
- It consists of three parts:
  - Part One - is the preparation for the audit (role-play);
  - Part Two - is the conduct of the audit (role-play);
  - Part Three - is the completion of an audit report together with any nonconformities and/ or opportunities for improvement that you have identified, on the forms provided.

TASK

- You have been asked to conduct an audit of Bangalore Business Solutions.
- The role-play focuses on a meeting with the top management to audit the organisation's continual improvement processes. You are looking for evidence that there is a planned and systematic approach to continual improvement in accordance with the requirements of ISO/IEC 27001:2022.
- Upon completion of the audit, prepare an audit report together with any nonconformities and/or opportunities for improvement that you have identified, on the forms provided.
- The role-play will focus on the ISMS at Bangalore Business Solutions

PART TWO: CONDUCTING THE AUDIT

- You will be expected to:
  - use any documents that you have prepared for this audit;
  - speak to top management in the organisation that you are auditing;
  - see any document in the organisation that you are auditing;
  - listen to responses from auditees and provide feedback;
  - record audit evidence;
  - ensure that confidentiality in respect of proprietary information is applied.
- You will also be expected to:
  - demonstrate the ability to manage meetings effectively;
  - demonstrate the ability to implement the audit plan, use work documents and to follow audit trails;
  - demonstrate the ability to build rapport with the auditee during the audit, including sensitivity to the needs and expectations of the auditee;
  - demonstrate the ability to manage audit interviews effectively, including the ability to formulate effective audit questions;
  - demonstrate the ability to collect and verify appropriate audit evidence, including appropriate sampling;
  - teams can make a “telephone appointment” with the person responsible for the ISMS at Bangalore Business Solutions to clarify any issues not immediately apparent from the information supplied.

OUTPUT

- Present your findings to the course Tutor.

TIME ALLOWED

- Role-play: 50 minutes.
- Feedback (to each team): 10 minutes

ACTIVITY EIGHT: AUDIT ROLE-PLAY: PART THREE: REPORTING THE AUDIT

PURPOSE

- To complete an audit report together with any nonconformities and/or opportunities for improvement.

PART THREE: REPORTING THE AUDIT

TASK

- Upon completion of the audit, prepare an audit report together with any nonconformities and/or opportunities for improvement that you have identified, on the forms provided.
- You will be expected to:
  - provide an accurate record of the audit;
  - correctly identify the processes audited;
  - identify the auditee's key representative;
  - state the audit conclusions on the audit objectives and scope;
  - reference the audit criteria against which the audit was conducted;
  - show the date that the audit was conducted;
  - accurately describe the audit findings;
  - summarise of the audit process including any obstacles encountered;
  - list any agreed follow-up action plans;
  - accurately describe any opportunities for improvement.

OUTPUT

- Be prepared to feedback your findings to the whole group.

TIME ALLOWED

- Activity: 50 minutes.
- Feedback: 10 minutes (each team).

APPENDICES

APPENDICES

Appendix 1: Terms and Definitions 212
Appendix 2: Example of an Internal Audit Programme Pro-forma 215
Appendix 3: Example of an Audit Plan Pro-forma 216
Appendix 4: Example of an Audit Checklist 217
Appendix 5: Example of a Completed Audit Checklist 218
Appendix 6: The “Turtle Diagram” 219
Appendix 7: Example of an Opening Meeting Checklist 220
Appendix 8: Example of a ‘CAR’ Form 221
Appendix 9: Example of an Internal Audit Report Pro-forma 222
Appendix 10: Example of a Third-party Certification Audit Report 223
Appendix 11: Closing Meeting Checklist 224
Appendix 12: CQI and IRCA Privacy Notice (GDPR) 225
Appendix 13: CQI Learner Privacy Notice (Online Exam) 226
Appendix 14: CQI and IRCA Online Exams: Guide for Learners 232
Appendix 15: CQI and IRCA Malpractice and Maladministration 246

APPENDIX 1: TERMS AND DEFINITIONS

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply. ISO and IEC maintain terminology databases for use in standardisation at the following addresses:

ISO Online browsing platform: available at https://www.iso.org/obp

IEC Electropedia: available at https://www.electropedia.org/

ASSET	
Anything that has a value to the organization	ISO/IEC 27002:2022
AUDIT	
Systematic, independent and documented process for obtaining objective evidence (3.8) and evaluating it objectively to determine the extent to which the audit criteria (3.7) are fulfilled	ISO 19011
AUDIT CRITERIA	
Set of requirements (3.23) used as a reference against which objective evidence (3.8) is compared	ISO 19011
AUDITOR	
IRCA grade of certificated Auditor for those who conduct full system audits as a member of an audit team and/or as a sole Auditor. Audits may be internal full system audits, second-party full system audits, or third-party audits for certification purposes	https://www.quality.org
ASSOCIATE AUDITOR	
IRCA grade of certificated Auditor who has passed an IRCA Auditor training course but does not meet the criteria for another grade.	https://www.quality.org

INTERNAL AUDITOR	
IRCA grade of certificated Auditor for those who conduct internal partial-system audits of a management system/s, or a supplier's management system. It is likely that you will not be a full-time Auditor and may only audit a few times each year	https://www.quality.org
LEAD AUDITOR	
IRCA grade of certificated Auditor for those experienced professionals who lead audits and audit teams. Applies to those conducting second or third party audits	https://www.quality.org
PRINCIPAL AUDITOR	
IRCA grade of certificated Auditor intended primarily for consultants who audit on their own. This grade is appropriate for senior audit professionals with an extensive and demonstrable history of conducting full system audits as Lead Auditors but who may no longer lead audit teams, or conduct audits on a regular basis Principal Auditors are often those who have moved to training, consultancy, or management roles. It offers highly skilled and experienced auditing professionals appropriate recognition without them being required to complete audits, which may no longer be a major part of their role	https://www.quality.org
INTERESTED PARTY	
Stakeholder person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity	ISO/IEC 27002:2022
OBJECTIVE	
Result to be achieved	ISO/IEC 27000:2018
OBJECTIVE EVIDENCE	
Data supporting the existence or verity of something	ISO 19011

PROCESS	
Set of interrelated or interacting activities which transforms inputs into outputs	ISO/IEC 27000:2018
REQUIREMENT	
Need or expectation that is stated, generally implied or obligatory	ISO 19011
RISK	
Effect of uncertainty on objectives (3.49)	ISO/IEC 27000:2018
RISK ANALYSIS	
process (3.54) to comprehend the nature of risk (3.61) and to determine the level of risk (3.39)	ISO/IEC 27000:2018
RISK ASSESSMENT	
Overall process (3.54) of risk identification (3.68), risk analysis (3.63) and risk evaluation (3.67)	ISO/IEC 27000:2018
RISK CRITERIA	
Terms of reference against which the significance of risk (3.61) is evaluated	ISO/IEC 27000:2018
RISK EVALUATION	
Process (3.54) of comparing the results of risk analysis (3.63) with risk criteria (3.66) to determine whether the risk (3.61) and/or its magnitude is acceptable or tolerable	ISO/IEC 27000:2018

APPENDIX 2: EXAMPLE OF AN INTERNAL AUDIT PROGRAMME PRO-FORMA

AUDIT KEY	AUDIT PLAN	
		Audit Scheduled
		Audit Completed and Satisfactory
		Audit Completed and Unsatisfactory
		Corrective Action Follow-up Audit Date
		Corrective Action Follow-up Audit Completed and Satisfactory

Process / Procedure / Department	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEPT	OCT	NOV	DEC

APPENDIX 3: EXAMPLE OF AN AUDIT PLAN PRO-FORMA

Organisation:			
Address:		**Date(s) On-site:**	
Lead Auditor:			
Team Member(s):			
Standard(s):			
Audit Language:			
Audit Scope and Observations:			
Criteria and Reference Docs:			

Date	Time	Auditor	Area / Department / Process / Function	Key Contact

Notes:

- Times are approximate and will be confirmed at the opening meeting prior to commencement of the audit.
- Auditors reserve the right to change, or add to the elements listed before, or during the audit depending on the results of on-site investigation.
- A private place for preparation, review and conferencing is requested for the Auditor's use.
- Please provide a light working lunch on-site each audit day.

APPENDIX 4: EXAMPLE OF AN AUDIT CHECKLIST

Audit Reference:		Sheet No. of	
Item No.	**Requirement**	**Activity Compliance** (Yes/No/Not Applicable)	**Comments/Remarks**

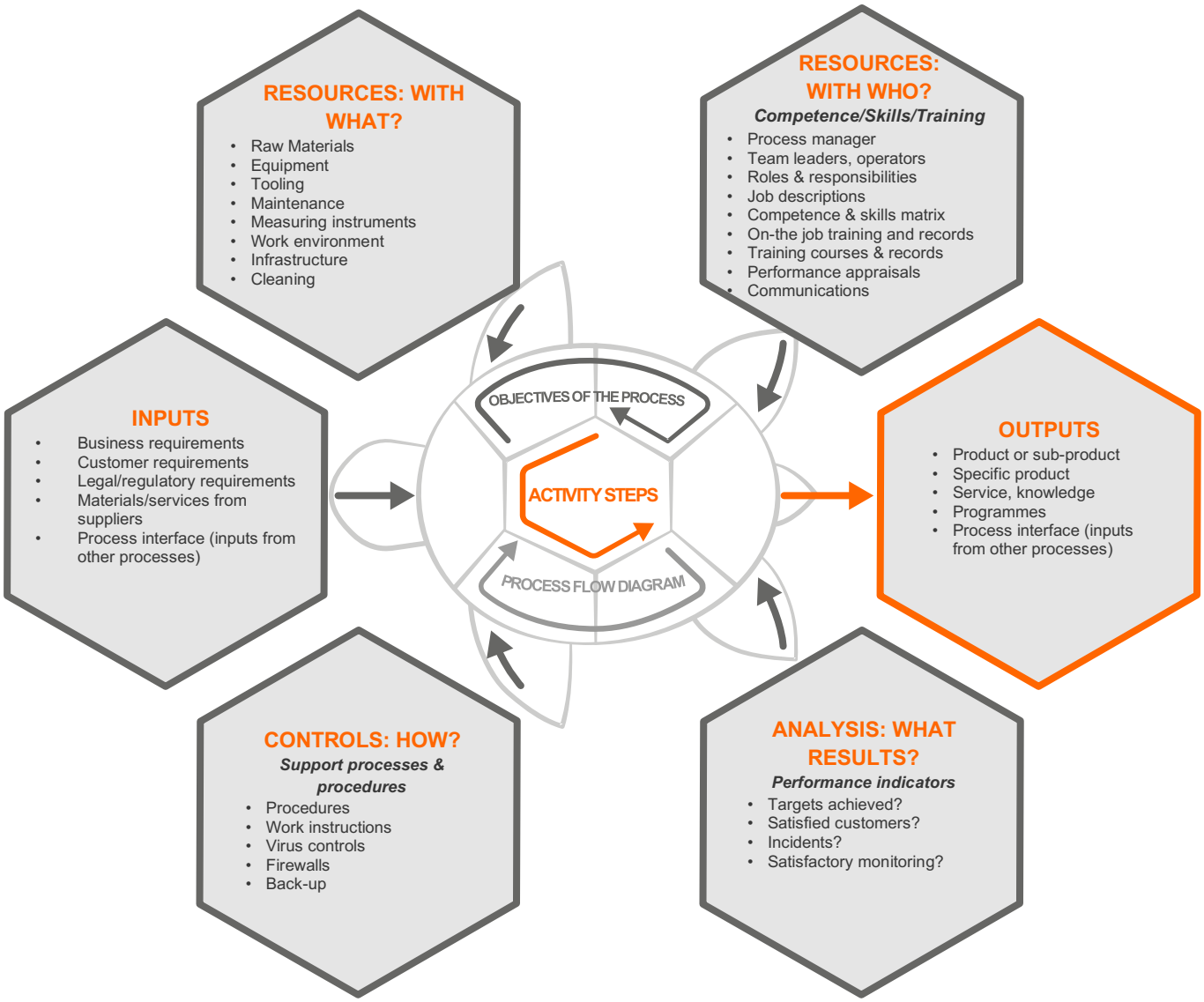
APPENDIX 5: EXAMPLE OF A COMPLETED AUDIT CHECKLIST

Audit Reference: Audit No.1 **Date: 10 / mm / yyyy** **Sheet No. 5 of 9**

Network Security Management: ISMS 089

Item No.	Requirement	Activity Compliance (Yes/No/Not Applicable)	Comments/Remarks
3.1	User access only to their limited services as authorised.	Yes	Verified, J. Washington, Server 6
	Appropriate authorisation methods used for remote users.		Verified, J. Washington, Server 6
3.3		Yes	
	Automatic equipment id. used for specific locations / equipment		Verified, J. Washington, Server 6
3.4		Yes	
	Physical and logical access to diagnostic and config. Ports controlled		Verified, M. Durban, Server 8
3.6		No	Verified, J. Washington, Server 6
	Connection capability of users sharing networks controlled.	Yes	Verified, M. Durban, Server 8
3.8	Shared networks have network routing controls.	Yes	Verified, J. Washington, Server 6
			Verified, M. Durban, Server 8
3.9			

APPENDIX 6: THE "TURTLE DIAGRAM"



APPENDIX 7: EXAMPLE OF AN OPENING MEETING CHECKLIST

Item No.	Item	
1)	Introduce self, position, organisation, experience. Introduce team.	
2)	Ask those at meeting to introduce themselves.	
3)	Confirm audit objectives, scope and criteria.	
4)	Confirm audit plan: ■ Date and time of the closing meeting. ■ Any interim meetings between the audit team and the auditee's management. ■ Any late changes.	
5)	Outline methods and procedures to be used to conduct the audit: ■ Classification of nonconformities. ■ Sampling technique. ■ Element of uncertainty inherent in all audits.	
6)	Establish formal communication links between the audit team and the auditee.	
7)	Confirm that during the audit, the auditee will be kept informed of audit progress.	
8)	Confirm that any resources and facilities needed by the audit team are available.	
9)	Confidentiality issues.	
10)	Procedures relating to relevant work safety, emergency and security.	
11)	Availability, roles and identity of any Guides.	
12)	Method of reporting including the classification of non-conformities.	
13)	Audit appeal system.	
14)	Any questions?	

APPENDIX 8: EXAMPLE OF A 'CAR' FORM

CORRECTIVE ACTION REQUEST MAJOR / MINOR				
COMPANY:				
JOB NO:	VISIT NO:	CAR NO:		
AUDITOR:		AUDIT DATE:		
COMPANY REPRESENTATIVE:				
PROCEDURE NO:		REF:		
ISSUE:		AREA/DEPT/FUNCTION:		
DETAILS OF NONCONFORMITY:				
SIGNED:	MAJOR CAR:		SIGNED:	
COMPANY:	PROPOSED:		AUDITOR:	
REPRESENTATIVE:			CLOSE OUT DATE:	
CORRECTIVE ACTION TAKEN TO PREVENT RECURRENCE:				
SIGNED:				
COMPANY REPRESENTATIVE:			DATE:	
ACCEPTANCE OF CORRECTIVE ACTION/COMMENTS:				
SIGNED:				
AUDITOR:			DATE:	
	MAJOR		MINOR	
	NOTIFY	CLOSE OUT	NOTIFY	CLOSE OUT
ASSESSMENT:	1 month	2 months	3 months	Next Surveillance
SURVEILLANCE/REASSESS:	2 weeks	1 month	3 months	Visit

APPENDIX 9: EXAMPLE OF AN INTERNAL AUDIT REPORT PRO-FORMA

INTERNAL AUDIT REPORT			
AUDITOR'S NAME		**AUDIT REPORT NUMBER**	
FUNCTION/ PROCESS AUDITED		**PREVIOUS AUDIT DATE AND RESULTS**	
DEPARTMENTAL REPRESENTATIVE		**DATE OF AUDIT**	
AUDIT SUMMARY:			
SIGNED (AUDITOR)		**DATE**	
SIGNED (DEPT. REPRESENTATIVE)		**DATE**	

APPENDIX 10: EXAMPLE OF A THIRD-PARTY CERTIFICATION AUDIT REPORT

Document	BY2-A84425
Visit No.	Initial
AUDIT REPORT	
Type of Audit	Initial
Date of Audit	19 & 20 January xxxx
Assessment Criteria	ISO/IEC 27001:2022
Lead Auditor	J. H. Soap
Auditors	M. W. Tate
Persons Contacted	Mr J. Tote Mr R. Cole

Summary of Audit:

J. Trown Ltd were visited on 19 & 20 January xxxx to carry out a non-site audit of their information security system against the requirements of ISO/IEC 27001:2022.

Prior to the visit a review of the documented system was carried out and found to be satisfactory.

The Company carries out a small engineering business, designing and manufacturing machine tools to order. The site is a model of good order and safety is a priority.

However, during the audit, three Minor nonconformances were raised; one on the risk assessment in reception area (CAR No. 1 refers) and two in purchasing (CAR No's 2 & 3 refer). In addition, two opportunities for improvement were made, concerning the communication of the IS system and the internal audit process. These were discussed at the closing meeting.

Details relating to the audit are contained in the main body of the report.

Conclusion	Registration is recommended.		
SIGNED (LEAD AUDITOR)		**DATE**	
SIGNED (GENERAL MANAGER)		**DATE**	

APPENDIX 11: EXAMPLE OF A CLOSING MEETING CHECKLIST

A closing meeting agenda will vary according to the type of audit conducted, but the following list, which is neither exhaustive nor prescriptive, contains typical items on a closing meeting agenda.

Item No.	Item	
1)	Distribute attendance list.	
2)	Restate purpose and scope.	
3)	Summary of good points within the management system.	
4)	Explain Major and Minor CARs.	
5)	Present NCRs.	
6)	Report on opportunities for improvement.	
7)	State decision and conclusion.	
8)	Explain significance of sampling technique.	
9)	Stress confidentiality.	
10)	Explain reporting and follow-up.	
11)	Explain CAR form completion.	
12)	Obtain client representative's signature on CAR.	
13)	Have Auditor log signed.	
14)	Obtain attendance list.	
15)	Thank the client and congratulate if appropriate.	

APPENDIX 12: CQI AND IRCA PRIVACY NOTICE (GDPR)

The Chartered Quality Institute (the CQI) has approved your training provider (SGS UK Ltd.) to deliver the certified course that you are attending.

During or after your course has finished, your training provider sends the CQI some information about you.

As a registered charity, the CQI is subject to the UK General Data Protection Regulation (UK GDPR), a UK law that gives you certain rights with respect to your personal data that is shared with the Institute.

The CQI process your data in order to:

- Provide you with a verifiable record at the conclusion of the course.
- Assess the provider and the training that you have received.

The data that is shared with us by your training provider (SGS UK Ltd.) includes your name, email address, the name of your tutor, the course in which you are registered, the date of your course and the results of final assessments that you have completed.

You are assigned a unique learner number when you register for a CQI and IRCA certified course. CQI retain your name, course and exam details, and this unique learner number in perpetuity, so that we can verify upon request, that you completed the course for which you have registered.

We use your name, email address and course information to send you a personalised email following the conclusion of your course, in which we ask you to give feedback on your experience with the course, your tutor and the training provider. We also ask you whether you are interested in receiving additional information from us about the quality profession, the CQI and IRCA and our products and services.

As a data subject you have certain rights under the GDPR including, for example, the right to access the data that the CQI and IRCA hold about you. To exercise your GDPR rights, you must contact the CQI either directly or through your training provider unless you are located in a European Union country when you must contact the CQI's EU representative – IT Governance Europe Limited at eurep@itgovernance.eu. Please ensure you reference 'CQI' in any correspondence you send to our representative.

The CQI can be reached directly at: Training@quality.org

APPENDIX 13: CQI LEARNER PRIVACY NOTICE (ONLINE EXAM)

INTRODUCTION

The Chartered Quality Institute (the CQI) has approved your training provider to deliver the certified course that you are attending.

During your course, your training provider will send us some information about you. This Privacy Notice explains what personal data will be collected and how the CQI will use your personal data.

Some of our courses require you to take an online exam. The CQI has partnered with ExcelSoft Technologies (referred to as ExcelSoft) to use their online assessment (**SARAS**) and their remote proctoring service (**Easy Proctor**) to deliver your online exams. We have a legally binding contract with ExcelSoft which requires them to keep personal data confidential. ExcelSoft will only process personal data on CQI's behalf and in accordance with our instructions.

CONTACT DETAILS

The CQI is subject to data protection laws, including the UK General Data Protection Regulation (**UK GDPR**). The UK GDPR gives you certain rights with respect your personal data. Unless otherwise specified below, you can exercise any of your rights with respect to our processing of your personal data by sending an email to privacy@quality.org or by writing to us at: **Privacy Officer, Chartered Quality Institute, Third Floor, 90 Chancery Lane, London, WC2A 1EU.** Please be aware that we may need to verify your identity before we can service your request.

We have appointed IT Governance Europe Limited to act as our European Union (EU) representative for data protection purposes. If you are based in the EU and you wish to exercise your rights under the EU General Data Protection Regulation (**UK GDPR**), or have any queries in relation to your rights or general privacy matters under EU data protection law, please email our Representative at europ@itgovernance.eu. Please include our company name in any correspondence you send to our Representative.

YOUR DATA PROTECTION RIGHTS

You are entitled to:

- **Access** the personal data that we hold about you. This is commonly known as a 'data subject access request'. There is generally no charge for making a data subject access request.
- **Rectify** personal data we hold about you that is inaccurate.
- **Withdraw your consent** to us processing your personal data.

In certain circumstances you are also entitled to:

- Ask us to **delete** the personal data we hold about you. Please note that we may not be able to delete all personal data that we hold about you, for example, because of our duties to regulate the quality profession under our Royal Charter.
- **Object** to our processing your personal data, depending on the legal basis under which we are processing your data.
- Ask us to **restrict** our processing of your personal data. For example, you may ask us to do this if you dispute the accuracy of your personal data, if you want us to restrict how we can use your data rather than deleting it, or if you have objected to our processing and we are dealing with your objection.
- Ask us to **transfer** your personal data to another person or organisation.

You can make a request by writing to us at the addresses given above.

You also have rights in relation to any **automated decision making**. You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces significant legal effects concerning you.

You can complain to the Information Commissioner's Office (**ICO**), the UK regulator for data protection: https://ico.org.uk/global/contact-us/.

WHAT TYPES OF PERSONAL DATA WILL BE COLLECTED?

The CQI will collect the following personal data:

- Your first and last names.
- Your email address.
- The training provider you are registered with.
- The course you are registered to take.
- Start and end dates of your course.
- Name of your tutor(s).
- Delivery method for your course.
- Country where you are located.
- Any request for a reasonable adjustment (CQI and IRCA online exam only).
- Your QI Unique Learner number if you already have one.
- Confirmation that you have given consent to your training provider for your data to be processed by the CQI and shared with ExcelSoft in accordance with CQI's Privacy Notice (CQI and IRCA only exam only).
- A photo of your face and a photo of your national government approved photo identification (CQI and IRCA only exam only).
- Video and audio recording of you and recording of your computer/laptop screen, taken during the exam (CQI and IRCA online exam only).
- Date of your exam (CQI and IRCA online exam only).
- Language of your exam (CQI and IRCA online exam only).
- Your proctoring result (CQI and IRCA online exam only).
- Your exam marks.
- Your overall exam result.
- Any request for special consideration (CQI and IRCA online exam only).
- Any appeal submission (CQI and IRCA online exam only).

HOW WILL MY PERSONAL DATA BE COLLECTED AND WHY DOES CQI NEED IT?

Your training provider will collect data relating to your name, email address, location, course details and assessment result (for courses that do not have an online exam). They will also collect data relating to learner requests for reasonable adjustments for courses with CQI and IRCA online exams. This data will be shared with the CQI.

The CQI will assign you a Unique Learner Number (ULN) which we will share with your training provider. We will retain your name, course details, exam result and your ULN in perpetuity, so that we can verify, upon request, that you completed the course for which you have registered.

We will also use the data to assess your provider and the quality of the training and assessment you received. We will use your name, email address and course information to send you a personalised email following the conclusion of your course, in which we ask you to give us feedback on your experience with the course, your tutor and the training provider. We will also ask you whether you are interested in receiving additional information from us about the quality profession, the CQI and IRCA, and our products and services.

In addition to the above, for learners taking a CQI and IRCA online exam:

The CQI will generate an assessment code for each learner taking an online exam. Your name, email address, ULN, assessment code and any reasonable adjustment request for extra time (if required) will be shared with ExcelSoft so that a username, passwords, and schedules for your practice questions and online exam can be generated and sent to you via email.

When you log onto SARAS to take your exam, you will be asked to take a photo of your face and a photo of your national government approved photo identification. This is to enable CQI to verify the identity of the person taking the exam. You will then be connected to ExcelSoft's remote proctoring tool Easy Proctor. Easy Proctor will video and audio record you for the duration of the exam, using the webcam and audio facility on your pc or laptop. It will also record the image displayed on the pc/laptop you are using for the exam. This data is collected to ensure that you are complying with CQI's online exam regulations.

In addition to the above, for learners taking a CQI and IRCA online exam:

At the end of the exam, you will be asked to complete a survey about your course and exam so that CQI can identify any areas for improvement. Easy Proctor will use artificial intelligence to analyse your exam video recording and will compare the photo of your face with the image of your photo identification and the video recording of the person taking the exam. The system will produce a proctoring report, which will highlight any anomalies and potential breaches of CQI's online exam rules. The report will be reviewed by the CQI to:

- Verify the person taking the exam is the same person who is registered for the exam.
- Confirm whether any anomalies flagged by Easy Proctor could amount to malpractice or could have adversely affected the learner's exam performance and result.

Once CQI has checked the proctoring report, your exam result, overall exam mark, exam marks by domain, date of exam and exam language will be sent from SARAS to CQI. Your training provider will download this data from CQI's portal and inform you of your exam result. CQI will use the data to monitor trends in exam performance across courses, training providers, tutors, and different languages, and to undertake quality improvement activities where necessary.

HOW WILL YOU STORE MY PERSONAL DATA?

The CQI will store your name, email address, ULN, course and exam information on our cloud-based server within the UK. We will retain this data in perpetuity, so that we can verify, upon request, that you completed the course for which you have registered.

ExcelSoft operates SARAS and Easy Proctor from cloud-based servers in the UK. All personal data processed by ExcelSoft will be stored securely for 90 days to allow any queries or appeals to be dealt with. ExcelSoft will delete this personal data after 90 days unless otherwise requested by CQI.

CQI will only ask ExcelSoft to retain your personal data for a longer period than stated in this Privacy Notice if we need it to deal with a complaint or appeal, or if we reasonably believe there is a prospect of a legal claim connected to your personal data.

QUERIES

If you have any questions about this Privacy Notice or about how we use your personal data, please contact us by email at: privacy@quality.org or by post to: **Privacy Officer, Chartered Quality Institute, Third floor, 90 Chancery Lane, London WC2A 1EU**.

APPENDIX 14 – CQI AND IRCA ONLINE EXAMS: GUIDE FOR LEARNERS

1. INTRODUCTION

Welcome to the CQI's learner guide for online exams. The purpose of this document is to provide you with all the information you need to take a CQI and IRCA online exam. It includes details of our regulations and requirements as well as advice on how to ensure your exam runs smoothly on the day.

CQI and IRCA online exams are delivered through an online assessment system called SARAS. You will have access to two SARAS portals – one for your practice questions and the other for your exam. The portal links are shown below:

https://practice.quality.org/TNA/PracticePortal

https://assessment.quality.org/TNA/TestPlayer/Login/Login.aspx

To log into your practice questions and exam you will need a 'username' and 'password'. You will receive two emails from the CQI - one with login instructions for the SARAS practice portal and the other with login details for the SARAS exam portal. If you haven't received the emails in your inbox, please check your junk email folder. If you provided your work email address to your training provider and you haven't received the emails, please also check with your IT team to see if the company's mail server has blocked the emails. If you have not received the emails by the end of your course, please contact your training provider.

Once you have logged into SARAS, you will have access to your learner homepage. This will either display details of your scheduled practice questions or your scheduled exam, depending on which portal you have logged into. Please check these details are correct. If any information is incorrect, please contact your training provider.

2. EXAM FORMAT

All Lead Auditor and Auditor Conversion online exams are structured as follows:

Lead Auditor Exam	
Exam Duration	1 hour 45 minutes (40 questions in total)
Exam content areas: ■ Section 1 – Concepts and principles of Management Standards and Systems	Recommended time for each section: 10 minutes (6 questions)
■ Section 2 – Audit concepts and Auditor responsibilities	10 minutes (6 questions)
■ Section 3 – Planning the audit	10 minutes (6 questions)
■ Section 4 – Conducting the audit	45 minutes (14 questions)
■ Section 5 – Reporting and closing out the audit	30 minutes (8 questions)

2. EXAM FORMAT, CONTINUED

Auditor Conversion Exam	
Exam Duration	1 hour 35 minutes (34 questions in total)
Exam content areas: ■ Section 1 – Concepts and principles of Management Standards and Systems ■ Section 2 – Planning the audit ■ Section 3 – Conducting the audit ■ Section 4 – Reporting and closing out the audit	Recommended time for each section: 10 minutes (6 questions) 10 minutes (6 questions) 45 minutes (14 questions) 30 minutes (8 questions)

The exam questions will be a mix of:

- Multiple choice (choose one correct answer)
- Multiple response (choose several correct answers)
- Fill in the blanks (drag and drop the correct words into the sentence)
- Matching (drag and drop responses to correctly match items)
- Sequencing (drag and drop responses to form the correct order)

The last two sections of the exam will include scenario questions related to conducting, reporting on, and closing out audits. You will be asked to evaluate the scenario presented to you and select the correct course(s) of action.

All questions will be computer-marked. **Once you have answered a question and clicked 'Next', you will not be able to navigate backwards to review or change your answer. This is a security measure to reduce the risk of cheating**.

The exams are open book, so you can refer to your notes from your training course. However, you are not permitted to use the internet to search for answers to questions. You will need access to a copy of the ISO management systems requirements standard associated with your course to answer some of the questions. The standards can be paper or electronic format.

To help you prepare for your exam, we have created 24 practice questions for the Lead Auditor exam and 20 for the Auditor Conversion exam. We strongly advise you take the practice questions before taking your online exam to familiarise yourself with the question types and how SARAS works.

You will have 30 days from the last day of your course to take your exam. The practice questions may be available earlier, depending on when your training provider uploads your details to the CQI.

3. REMOTE PROCTORING

CQI and IRCA online exams are invigilated remotely, using Easy Proctor. The system will:

(a) Take an image of your photo identification (photo ID) and your face.

(b) Record you for the duration of your exam using your webcam and microphone.

(c) Record your computer screen for the duration of your exam.

Details of acceptable forms of photo identification can be found below in the section 'Online Exam Regulations'.

Once you have completed the exam, Easy Proctor will compare your photo ID with your facial image to verify you are the same person and will analyse the recording of your exam session for any anomalies, such as unexpected sounds, movements, objects, or people. It will then flag these incidents to the CQI for further investigation.

4. REASONABLE ADJUSTMENT

If you need extra support or time to take the exam due to a physical or learning disability or require a female CQI member of staff to review your proctoring video recording for religious reasons, you must notify your training provider as soon as possible and well in advance of taking your exam so they can submit a reasonable adjustment request to the CQI on your behalf. If you are taking your exam in English, and English is not your first language, you can request an additional 30 minutes. If you are unable to take your exam within the scheduled 30 day period, e.g. due to illness, you can request an extension to your exam schedule. Please refer to Appendix 1: CQI's Reasonable Adjustments Policy, for more information.

5. EQUIPMENT AND SYSTEM REQUIREMENTS

To take the exam you will need:

5.1 - A computer or laptop with a working webcam and microphone ***(please note, smart phones, iPads/tablets, touchscreens, and 2-in-1/hybrid laptops with front and rear cameras are not permitted)***.

- You may use a second screen if you need to access a digital version of the standards and/or your course notes.
- If using a laptop, we recommend you connect to an external monitor to optimise your online exam experience.

5. EQUIPMENT AND SYSTEM REQUIREMENTS, CONTINUED

- **5.2** - A system that meets the following minimum requirements:

	Minimum Windows operating requirements	Minimum Mac operating system
Hardware		
Available free disk space	15 GB	15 GB
Display resolution	Best view in 1280 x 1024	Best view in 1280 x 1024
Network adapter	1 Gbps Network Interface Card	1 Gbps Network Interface Card
Software		
Operating system	Windows 8.1 or above (excluding Windows 10S)	Catalina (10.15.5 to 10.15.7) Mojave (10.14 to 10.14.6) Sierra (10.12 to 10.12.6) Big Sur (11.0 only)
Browsers	Chrome version 85+. Firefox version 85+ and Microsoft Edge version 91+ are permitted but **Chrome is the preferred browser**.	Chrome version 85+

5.3 - **Continuous, stable internet connection**. Cellular connection and/or VPN are not suitable due to their unreliability and unstable nature. A wired connection is ideal, but a strong and stable Wi-Fi connection should be sufficient.

5.4 - To enable video proctoring, the following bandwidth is required:

Camera Resolution	Bandwidth Required
1 megapixel (1280*720)	5-7 megabits per second (Mbps)
2 megapixel (1920*1080)	7-10 Mbps
4 megapixel (2560*1440)	10-12 Mbps

NB: the bandwidth requirement for HD cameras increases between 10-12 Mbps.

5.4, continued

The landing pages for the practice and exam portals contain the following tools:

- System Check Tool
- Test Your Camera
- Test Your Microphone

The System Check Tool also has a link to an Audio and Video Streaming test. We strongly recommend that you use these tools to check that your laptop or computer meets the minimum requirements, and your webcam and microphone are working correctly.

https://practice.quality.org/TNA/PracticePortal

https://assessment.quality.org/TNA/TestPlayer/Login/Login.asp

Please test the device that you are going to use for your exam. Do not assume, for example, that if your work laptop meets the IT requirements, then your personal laptop will too.

It's a good idea to run the system test at about the same time of day you expect to take your exam to get a better feel for the internet connectivity you are likely to have. If you run the system test at 10:00pm and take your exam at 2:00pm, the bandwidth available may be quite different.

6. ONLINE EXAM REGULATIONS

Please read the following regulations carefully. Before you can start your exam, SARAS will ask you to confirm that you have read, understood, and accept CQI's regulations for online exams. If you decline, you will not be able to take the exam.

Photo Identification

At the start of the exam you will be required to show photo identification so that we can verify the identity of the person taking the exam. You must present one of the following forms of government-issued identification:

- Current valid passport
- Current photocard driving licence
- National identification card

If you do not have any of the above, please contact the CQI at assessment@quality.org as soon as possible to discuss alternative arrangements. Learners who do not present valid photo identification may be disqualified.

Exam Conditions

You can take your exam in any location, provided it meets the following requirements:

- Quiet: Somewhere where you will not be disturbed by others or by external noise, e.g. building work or traffic noise.
- Well lit: Do not sit in front of a window or other bright light. If you are backlit, draw shades or curtains and/or turn off lights behind you.
- Private: Make sure others cannot see your computer or monitor
- Access to a power socket: So you can plug in your laptop to ensure it does not run out of battery during the exam

Learner Conduct

You must always behave professionally and honestly during the exam.

- Your face must be uncovered for the duration of the exam. If you wear a headscarf, you must show your ears. Hoodies, hats, and sunglasses are not permitted.
- Your webcam and microphone must remain switched on for the duration of the exam. When using your webcam, please ensure that your head is positioned in the centre of the camera image, facing the camera head on and that the webcam is not pointing to the side, above or below your face.
- You must remain silent for the duration of the exam.
- You are permitted a 10 minute break. You must use the ‘Take a break’ button so that it is logged as an official break for proctoring purposes. If you leave the room at any other time, the proctoring system will record your absence and flag to CQI for further investigation.
- Do not bring any food into the exam room. You are allowed to bring a drink but at your own risk as spillage may compromise the functionality of your computer and therefore your ability to complete the exam.
- Smoking and vaping are not permitted.
- You must not attempt to communicate either in person or electronically with anyone inside or outside the exam room.
- Do not bring any unauthorised electronic devices into the exam room. This includes mobile phones, iPads/tablets, smart watches, headphones, and earphones. The only electronic equipment you are permitted to use is the device you are using to take your exam.

Learner Conduct, continued

You must not do anything that could infringe CQI's intellectual property rights and/or compromise the confidentiality and integrity of CQI online exams. Examples of misconduct include but are not limited to:

- Providing access to, disclosing, distributing, copying, photographing, recording, downloading, and transmitting any exam questions, answers or content in any form or by any means.
- Misrepresenting your identity or impersonating another individual during the exam.
- Being in possession of any non-authorised items whilst taking the exam such as mobile phones, electronic devices, smart watches, headphones, earphones.
- Helping others with the exam or receiving assistance either online or in person during the exam.
- Using the internet to research answers to questions.
- Turning off your webcam and/or microphone, obscuring your face with a face covering, positioning your webcam so that there is not always a clear image of your face.
- Continuously looking around in any direction or looking at your wrist, CQI will investigate any potential breaches of the Online Exam Regulations in accordance with our Malpractice and Maladministration policy. If you are found to have committed malpractice, CQI reserves the right to void your exam result and disqualify you from future CQI exams either for a fixed period or indefinitely.

7. EXAM RESULTS

Once you have completed your exam, the CQI will review the findings from your proctoring recording and if there are no issues, the results will be available for your training provider to download within 10 UK working days. If you have not received your results within 14 working days of taking your exam, please contact your training provider.

8. SPECIAL CONSIDERATION

You can submit a request for special consideration if you feel that your exam performance was adversely affected by an event outside of your control either during or just prior to taking your exam e.g. death of a relative, illness. Please refer to Appendix 2 CQI's Special Consideration Policy for more information.

9. APPEALS

An appeal considers whether the correct policies and processes have been followed and applied fairly. You can submit an appeal in relation to the following:

- Appeal against a 'Fail' result
- Appeal against a malpractice decision
- Appeal against a decision made in relation to a reasonable adjustment or special consideration Please refer to Appendix 3 CQI's Appeals Policy for more information.

10. EXAM CHECKLIST

- At least 3 days before taking your exam:
- Check you have the correct IT equipment and systems.
- Check your webcam and microphone are working properly.
- Log into SARAS to confirm your username and password are working and that you are registered for the correct exam.
- Check the suitability of your chosen exam location.
- Check you have the required Photo ID and ISO standards.
- Inform colleagues, family and friends of the date and time you intend to take your exam and advise them that you cannot be interrupted during the exam and will not be available to respond to emails/messages/phone calls etc.
- Take the 'practice' questions.

On the day of your exam:

- Run the systems check again and test your webcam and microphone to confirm they are still working correctly.
- Check you have your photo ID and ISO standards.
- Disable your pop-up blocker to enable the exam software to launch.
- Turn off any auto updating applications if possible.
- If you are using freeware anti-virus tools, please switch them off. If your exam is blocked by an antivirus tool, please go to the antivirus setting and enable the exam software to run.

On the day of your exam, continued:

- Make sure you are taking the exam in a quiet, well-lit environment.
- Remove any smart phones/smart watches/cameras/ tablets/earphones/ear pods and other electrical devices from your exam environment.
- Remind others that you do not want to be disturbed during the exam.
- Grab a drink.

When you are ready, log into your learner home page on SARAS and click ‘Start Exam’.

SARAS will ask you to hold up your Photo ID to your webcam and take a picture. The picture of your ID must clearly show your name and photo and fit within the red frame on the screen. You will have a chance to review the picture before submitting it to SARAS, so please check all the required information is visible. Next SARAS will ask you to take a photo of your face. Please ensure that your head and face are not covered by a hat or face covering, that you are looking directly at the camera and that your face fits within the oval red frame on the screen.

When you are satisfied with the quality of both images, submit your photos. You will then see some instructions on how to navigate the exam and allocate your time. You will also be asked to accept CQI’s Online Exam Regulations. Once you click ‘accept’ you can then start your exam. If you have any problems during the exam, please contact the CQI at assessment@quality.org. Please note, this inbox will only be monitored during UK working hours.

Good luck! And don’t forget to complete the Learner Experience Survey at the end of the exam.

APPENDIX 1: CQI AND IRCA ONLINE EXAMS: REASONABLE ADJUSTMENT POLICY

A reasonable adjustment is an action that helps reduce the effect of a disability or difficulty that would otherwise place a learner at a substantial disadvantage in an online exam situation. Examples of reasonable adjustments include:

- Extending the duration of the exam - for example if a learner is taking an exam in English and English is not their first language or they have a learning disability, CQI can extend the exam duration by 30 minutes.
- Providing assistance during the exam such as a reader - CQI's online assessment system supports NVDA and JAWS screen reader software.
- Arranging for a female proctor to check the identification and proctoring recording of a female Muslim learner.
- Extending the exam schedule – for example if a learner cannot take their exam within the 30 days exam window due to illness.

An adjustment will not be approved if it involves unreasonable costs, timeframes or affects the security or integrity of the exam. This is because the adjustment is not 'reasonable.' A reasonable adjustment must not give the learner an unfair advantage over other learners taking the same or similar exams.

Prior to the start of the course, you should discuss any reasonable adjustment needs with your training provider. Depending on the reason for the adjustment, your training provider may ask you to provide supporting medical evidence to confirm your request is valid.

If you are taking your exam in English and you require extra time because English is not your first language, your training provider will inform us when they send us your registration details. For all other reasonable adjustment requests, your training provider will complete a Reasonable Adjustments Request Form and email the form to CQI.

CQI will acknowledge the reasonable adjustments request and will process the request within 2 UK working days. CQI will email your training provider to confirm whether the reasonable adjustment has been approved and what action has been taken. Your training provider will then inform you of the outcome.

If extra time has been requested, the duration of your exam will be increased on the exam schedule shown on the learner homepage of your SARAS Exam portal. If the extra time is not showing, please contact CQI at assessment@quality.org.

If you are unhappy with the outcome of your reasonable adjustment request, you have the right to appeal (see Appendix 3 CQI and IRCA Online Exams: Appeals).

APPENDIX 2: CQI AND IRCA ONLINE EXAMS: SPECIAL CONSIDERATION POLICY

A learner may apply to CQI for special consideration if they feel their performance during their exam was significantly affected by:

- An unexpected or temporary illness, injury or other indisposition.
- An event outside of their control such as a bereavement just before the exam or a serious disturbance during the exam.

Special consideration will not be given for the following circumstances:

- Unexpected events which did not occur near to the day of the exam.
- Issues caused by the learner's own actions e.g. hardware, software or internet-related problems due to the learner not complying with CQI's online exam requirements.
- Issues caused by the learner not sufficiently preparing for the exam e.g. by not attending all of the course or not completing all the requirements.

In addition, learners who have received a reasonable adjustment will not be entitled to receive special consideration for the same circumstances.

Special consideration may include a small post-exam adjustment to a learner's mark or the offer of a free resit, depending on the circumstances and level of difficulty faced by the learner. A free resit will only be offered to learners if their performance has been impaired due to a significant technical problem caused by CQI's online assessment system. Issues due to learner equipment failure or internet related issues will not be considered.

Special consideration must not give the learner an unfair advantage neither should it mislead stakeholders regarding the learner's achievement. A learner's result must reflect their achievement in the exam and not their potential ability. The maximum adjustment given will be 5% of the total marks available for the exam. This is to protect the standard and integrity of CQI's exams.

If you have failed and feel that your exam performance was affected by one of the reasons listed above, you can apply for special consideration. Learners are strongly advised to discuss the request with their training provider prior to submission, as a learner who has achieved a low mark will not have their marks adjusted to such an extent that they move from a Fail to a Pass and may not be eligible for a free resit.

If you decide to apply for special consideration, you must complete a CQI and IRCA Online Exams: Special Consideration Request Form (available from CQI's website and your training provider) and email the completed form and supporting evidence to assessment@quality.org within 5 working days of taking your exam. CQI will acknowledge the email and will process the special consideration request within 10 UK working days.

CQI will email you and your training provider to confirm whether the special consideration request was accepted and what action has been taken. If you are unhappy with the result, you have the right to appeal (see Appendix CQI and IRCA Online Exams: Appeals Policy).

APPENDIX 3 CQI AND IRCA ONLINE EXAMS: APPEALS POLICY

An appeal is a formal request for a review of a decision. An appeal considers whether the correct policies and processes have been followed and applied fairly. A learner may make an appeal to CQI in relation to the following:

1. Appeal against a 'Fail' result.
2. Appeal against a malpractice decision.
3. Appeal against a decision made in relation to a reasonable adjustment or special consideration.

Appeal against a 'Fail' result

An appeal may be submitted if the learner considers that:

- An error has occurred in relation to the marking and/or grading process.
- There is an issue with the wording or translation of one or more questions which has adversely affected the learner's result.

Please note, we will not accept appeals against a 'Fail' result in relation to problems with internet connectivity or pc/laptop hardware or software issues. Learners should follow the Special Consideration process if they experienced technological problems which they feel affected their performance during the exam.

Appeal against a malpractice decision

Malpractice means 'any deliberate activity, neglect, default or other practice that compromises or could compromise the assessment process, the integrity of a CQI and IRCA certified course, the validity of a result or certificate, or the reputation and credibility of the CQI and CQI and IRCA certified courses'. Examples of malpractice by a learner in relation to online exams include:

- Being in possession of confidential material e.g. exam questions and answers in advance of, and/or during, the exam.
- Providing access to, disclosing, distributing, copying, photographing, recording, downloading, and transmitting any exam questions, answers, or content in any form or by any means.
- Misrepresenting their identity or impersonating another individual during the exam.
- Arranging for someone else to sit the exam on their behalf.
- Helping others with the exam or receiving assistance either online or in person during the exam.

Appeal against a malpractice decision, continued

- Copying another learner's answers or knowingly allowing a learner to copy from their work.
- Inappropriate behaviour during the exam e.g. using offensive language.
- Being in possession of any non-authorised items whilst taking the exam such as mobile phones, electronic devices, smart watches, headphones, and earphones. Possession of such devices will be considered as malpractice whether or not the learner uses them.
- Turning off their webcam and/or microphone, obscuring their face with a face covering, positioning their webcam so that there is always not a clear image of their face.

Malpractice may be identified during an analysis of the learner's proctoring recording or due to information that CQI receives either before or after the exam. All learners found guilty of malpractice will receive a 'disqualified' result, regardless of whether they have passed or failed the exam and will be provided with details of the malpractice. CQI reserves the right to disqualify learners from future CQI exams either for a fixed period or indefinitely.

Appeal against a reasonable adjustment or special consideration decision

CQI recognises that some learners may be prevented from demonstrating their achievement due to:

- A permanent or long-term disability, learning difficulty or medical condition.
- A temporary disability, illness or indisposition immediate to or at the time of the exam.
- Circumstances at the time of or during the exam.

Please see CQI's Reasonable Adjustment and Special Consideration policies for further details. Learners have the right to appeal CQI's decision in relation to these requests.

Process

If you wish to appeal you are strongly advised to discuss your case with your training provider prior to making a submission. If you decide to make an appeal, you must complete the CQI and IRCA Online Exams: Appeals Submission Form (available from CQI's website and your training provider). You must email the form and supporting evidence to assessment@quality.org within 14 calendar days of receiving your exam result or outcome of your reasonable adjustment or special consideration request.

Process, continued

CQI will acknowledge the email and will process the appeal as follows:

- Reasonable adjustment appeal - within 2 UK working days.
- Special consideration appeal - within 10 UK working days.
- 'Fail' result appeal - within 10 UK working days.
- Malpractice appeal - within 10 UK working days.

Appeals will be reviewed by a CQI senior member of staff who has not previously been involved in the case and has no personal interest in the outcome.

The person investigating the appeal will re-examine the evidence used to make the original decision and any additional evidence provided by the learner. They will consider whether CQI has applied its processes consistently, properly and fairly in arriving at the decision. For appeals relating to malpractice, the reviewer will consider, on the balance of probabilities, whether there was sufficient evidence to support the malpractice finding and how appropriate the decision was in light of precedents and any additional information provided by the learner.

CQI will email you and your training provider to confirm whether the appeal has been upheld or rejected, and what follow-up action has been taken. No further appeals will be accepted

APPENDIX 15: CQI AND IRCA MALPRACTICE AND MALADMINISTRATION

MALPRACTICE

- Malpractice means 'any deliberate activity, neglect, default or other practice that compromises or could compromise the assessment process, the integrity of a CQI and IRCA Certified Course, the validity of a result or certificate, or the reputation and credibility of the CQI, and CQI and IRCA Certified Courses'.
- Malpractice includes issues such as deliberate falsification of records in order to claim certification, cheating in examinations and unethical conduct by ATP staff, tutors, branches or subcontractors.
- Malpractice also includes failure by the ATP to:
  - Investigate allegations and suspected malpractice and notify the CQI promptly
  - Co-operate with the CQI's investigations

MALADMINISTRATION

- Maladministration means 'any actions, neglect, default or other practice that results in an ATP not complying with the CQI's ATP criteria and requirements as specified in the ATP Quality Handbook'. This could be due to mismanagement, incompetence or inefficiency.
- Examples of **malpractice** by learners are:
  - arranging for someone else to sit a CQI and IRCA examination on his/her behalf;
  - impersonation of another learner;
  - being in possession of confidential material in advance of the examination, e.g. examination question paper, model answer or marking guidance;
  - being in possession of materials not permitted in the examination room, possession of such materials will be considered malpractice whether or not he learner uses them;
  - communicating with other students in the examination room in breach of CQI examination regulations;
  - copying the work of another student or knowingly allowing another student to copy from his/her work;

MALADMINISTRATION, CONTINUED

- working collaboratively with any other student(s) by whatever means during examinations;
- including inappropriate, offensive material in examination scripts;
- plagiarism or misrepresentation of learner's work;
- failure to adhere to the published AQI examination regulations;
- failure to adhere to instructions given by examination invigilator in relation to examination regulations, e.g. continuing to work beyond the allotted examination time, refusing to hand in the examination script and/or examination paper when requested, not adhering to warnings relating to conduct during the examination;
- disruptive behaviour (including offensive language and aggressive/violent conduct) in the training and examination venue;
- tampering with, or forgery of results, documentation, including certificate.

- Examples of **malpractice** by staff, tutors, invigilators and markers working for an ATP, a branch or a subcontractor are:
  - Breach of security

    Any act which breaks the confidentiality of examination question papers or materials or the confidentiality of learners' examination scripts. This could involve:
    - failure to keep examination question papers, marking schemes or scripts secure before, during or after an examination;
    - discussing or revealing in public (e.g. posting on social media) secure information relating to CQI and IRCA examinations;
    - tampering with learners' examination scripts.

MALADMINISTRATION, CONTINUED

- Deception

  Any act of dishonesty in relation to examination scripts, such as:

  - inventing or changing examination marks when there is no evidence of learner achievement to justify the marks being given;
  - when marking examination scripts, not reporting suspected incidents of malpractice by a learner to the ATP;
  - entering fictitious learners for examinations or otherwise subverting the assessment or certification process with the intention of financial gain.

- Improper assistance to learners:

  - knowingly allowing an individual to impersonate a learner;
  - allowing a learner to possess and/or use materials not permitted in the examination room;
  - allowing learners to communicate with each other during an examination in breach of CQI regulations;
  - allowing a learner to copy another learners' work or allowing a learner to let his/her own work to be copied;
  - allowing learners to work collaboratively during an examination;
  - advising and/or assisting a learner with his/her examination answers;
  - allowing a learner to work beyond the allotted examination time unless a time extension has been agreed in advance in accordance with CQI examination regulations;
  - damaging a learners' work;
  - disruptive behaviour in the training and examination venue;
  - leaving learners unsupervised during an examination;
  - divulging any information relating to a learners' examination performance and/or result to anyone other than the learner him/herself;
  - tampering with, or forgery of, results files and/or associated documentation.

MALADMINISTRATION, CONTINUED

- Failure to co-operate with an investigation:
  - failure to make available information reasonably requested by the CQI in the course of an investigation, or in deciding whether an investigation is necessary;
  - failure to respond to an instruction from the CQI to investigate an allegation or suspected case of malpractice or maladministration;
  - failure to investigate or provide information according to agreed deadlines;
  - failure to report all suspicions of malpractice.

- Examples of **maladministration** by staff, tutors, invigilators and markers working for an ATP, a branch or a subcontractor:
  - not using current examination papers, marking schemes and documentation;
  - failure to train adequately those invigilating examinations;
  - failure to ensure that examination venues conform with the CQI's requirements;
  - failure to standardise and moderate tutor marking;
  - failure to keep accurate learner records;
  - failure to upload accurate learner data to the CQI;
  - failure to store and despatch certificates securely and in a timely manner.
  -

CQI and IRCA Certified Training

We hope you enjoyed your course!

You will be contacted by the CQI and IRCA for feedback on the course and your Approved Training Partner.

Completing this short survey will help to ensure the continuing high standards of these courses.

The CQI and IRCA offer a range of services to support you throughout your career. For more information, please visit **www.quality.org**



CONTACT SGS ACADEMY

Contact us today to find out how the SGS Academy can help fulfill your training requirements.


www.sgs.com


www.facebook.com/SGS/


www.sgs.com/twitter


www.sgs.com/linkedin


training@sgs.com



WWW.SGS.COM

© SGS Group Management SA – 2018 – All rights reserved - SGS is a registered trademark of SGS Group Management SA

WHEN YOU NEED TO BE SURE

SGS