

Вспомогательный материал к упражнениям

STUDENT NOTES

ABOUT THIS COURSE

COURSE OBJECTIVES

This course has been developed to meet the criteria for an Information Security Lead Auditor Course.

The Learning Objectives of the course can be summarized as follows:

- ⇒ To gain the knowledge regarding:
 - The purpose and business benefits of an information security management system, of information security management systems standards, of management system audit and of third-party certification.
 - The role of an auditor to plan, conduct, report and follow up an information security management system audit in accordance with ISO 19011 (and ISO 17021 where appropriate).
- ⇒ To gain the skills required to:
 - Plan, conduct, report and follow up an audit of an information security management system to establish conformity (or otherwise) with ISO/IEC 27001 (with ISO/IEC 27002) in accordance with ISO 19011 (and ISO 17021 where appropriate).

OUR METHODS

The most important thing to us is that at the end of the week you feel that you have learned something worthwhile and you alongside with us, during all the steps of the way, have been prepared and are in the best possible position and frame of mind to pass your exam and go on to become a good auditor.

To achieve the above, you'll find that we apply an approach of learning by doing, review, discussion, team work and allowing you to have the occasional laugh along the way. The most important thing you need to know is that it is your tutor's job to make sure you learn, not yours, but you must play your part by speaking up if there's anything you are having difficulty with. Your tutor will then need to work a bit harder to think of a way to help you. Don't be afraid to ask questions.

STUDENT NOTES

This course has been developed around the 2022 issue of the ISO/IEC 27001 standard. ISO 27001:2013 is the first version of ISO 27001 that has adopted the "Annex SL" Common Management System structure.

AN OVERVIEW OF THE ANNEX SL COMMON FORMAT FOR MANAGEMENT SYSTEMS

Annex SL is part of a much larger document (publicly available, free of charge) **ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures Specific to ISO**. The document covers a very wide range of issues relating to the development of ISO procedures. Annex SL is the part of that wider document that relates specifically to the Development (Appendix 1) and the Format & Structure (Appendix 2) of ISO standards.

Purpose and Structure of the Annex SL Format

The adoption of the Annex SL format for ISO management system standards recognises that a common format offers advantages to the user community, and there has been, for some time, a growing demand that, so far as is possible, the ISO management system standards have similar structures.

The common format seeks to achieve the following objectives:

- Market Value Any management system should meet the needs of, and add value for, the primary users and interested parties
- **Compatibility** Compatibility between various standards should be maintained
- Topic Coverage Any standard should have sufficient application coverage so as to eliminate or minimise the need for sector specific variations
- Free Trade Any standard should permit the free trade of goods and services of cultures and of every size. An MSS should not prevent organizations from competitively adding to or differentiating from others, or enhancing their management systems beyond the standard
- Applicability of Conformity Assessments The market needs for first-, second- or third-party Conformity assessment, or any combination thereof, should be assessed. The resulting standard should clearly address the suitability of use for conformity assessment in its scope. A standard should facilitate joint audits
- **Exclusions** A standard should not include directly related product (including services) specifications, test methods, performance levels (i.e. setting of limits) or other forms of standardization for products produced by the implementing organization
- Ease of Use It should be ensured that the user can easily implement one or more standards. A standard should be easily understood, unambiguous, free from cultural bias, easily translatable, and applicable to businesses in general.

STUDENT NOTES

Consequently, and in summary, the aim was to develop a common format that would improve user-friendliness and relevance, make integration easier (important, for example, for organisations operating Integrated Management Systems with multiple certifications in place) and to make conformity assessments more consistent and relevant. All standards adopting the Annex SL format will therefore have a common high-level structure and core text.

Common Clause Structure

The clause structure of all standards adopting the Annex SL format is as follows;

- 1. Scope
- 2. Normative References
- 3. Terms and definitions
- 4. Context of the Organisation
- 5. Leadership
- 6. Planning
- 7. Support
- 8. Operation
- 9. Performance evaluation
- 10. Improvement

The content and implications of the significant clause requirements will be addressed in turn and in detail later in this document.

Annex SL Common Terms and Definitions

The purpose of clearly defined and understood terms and definitions can't be understated. Their purpose is to calibrate the use of the standard and reduce the potential for variation. It is important to remember that many of the words used in ISO management system standards are also used in everyday speech, and the context in everyday use of the same word or term may differ from the Annex SL definition.

The OED definitions of words may well be different too, so it is important that we understand that, when using ISO standards that follow the Annex SL structure (such as ISO 9001:2015 and ISO 14001:2015) the Annex SL definition applies. The table below contains the Annex SL definitions.

STUDENT NOTES

TERM	DEFINITI ON		
Organisation	Person or group of people that has its own functions with responsibilities, authorities and		
	relationships to achieve its objectives		
Interested Party (or stakeholder)	Person or <i>organization</i> that can affect, be affected by, or perceive itself to be affected by a decision or activity		
Requirement	Need or expectation that is stated, generally implied or obligatory		
Management System	Set of interrelated or interacting elements of an <i>organization</i> to establish <i>policies</i> and <i>objectives</i> and <i>processes</i> to achieve those objectives		
Top Management	Person or group of people who directs and controls an organization at the highest level		
Effectiveness	Extent to which planned activities are realized and planned results achieved		
Policy	Intentions and direction of an <i>organization</i> , as formally expressed by its <i>top</i> management		
Objective	Result to be achieved		
Risk	Effect of uncertainty		
Competence	Ability to apply knowledge and skills to achieve intended results		
Documented Information	Information required to be controlled and maintained by an <i>organization</i> and the medium on which it is contained		
Process	Set of interrelated or interacting activities which transforms inputs into outputs		
Performance	Measurable Result		
Outsource	Make an arrangement where an external <i>organization</i> performs part of an organization's function or <i>process</i>		
Monitoring	Determining the status of a system, a process or an activity		
Measurement	Process to determine a value		
Audit	Systematic, independent and documented <i>process</i> for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled		
Conformity	Fulfilment of a requirement		
Non-conformity	Non-fulfilment of a requirement		
Corrective Action	Action to eliminate the cause of a nonconformity and to prevent recurrence		
Continual Improvement	Recurring activity to enhance performance		

STUDENT NOTES

THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Throughout this course we'll be using a number of terms and definitions and we need to apply them correctly in the context of this course. What that means is that we use the terms as defined within (for this course at least) ISO 27000 and ISO 19011.

The definition for "Information Security Management System" (ISMS) can be found in ISO 27000. It is:

"Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security"

What is an ISMS?

An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS.

The following fundamental principles also contribute to the successful implementation of an ISMS:

- awareness of the need for information security;
- assignment of responsibility for information security;
- incorporating management commitment and the interests of stakeholders;
- enhancing societal values;
- risk assessments determining appropriate controls to reach acceptable levels of risk;
- security incorporated as an essential element of information networks and systems;
- 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 27000 Family

The ISMS family of standards consists of inter-related standards, already published or under development, and contains a number of significant structural components. These components are focused on:

- standards describing ISMS requirements (ISO/IEC 27001)
- certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001; and
- additional requirement framework for sector-specific implementations of the ISMS (ISO/IEC 27009)



STUDENT NOTES

Other documents provide guidance for various aspects of an ISMS implementation, addressing a generic process as well as sector-specific guidance.



Each of the ISMS family standards is described below by its type (or role) within the ISMS family of standards and its reference number.

- ISO/IEC 27000 Standard describing an overview and terminology
- **ISO/IEC 27001** Standard specifying requirements, Information security management systems
- ISO/IEC 27006 Standard specifying requirements, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27009 Standard specifying requirements, Sector-specific application of ISO/IEC 27001 -Requirements
- ISO/IEC 27002 Standard describing general guidelines, Code of practice for information security controls
- ISO/IEC 27003 Standard describing general guidelines, Information security management Guidance
- ISO/IEC 27004 Standard describing general guidelines, Information security management Monitoring, measurement, analysis and evaluation
- ISO/IEC 27005 Standard describing general guidelines, Information security risk management
- ISO/IEC 27007 Standard describing general guidelines, Information, Guidelines for information security management systems auditing
- ISO/IEC TR 27008 Standard describing general guidelines, Guidelines for auditors on information security controls
- ISO/IEC 27017 Standard describing sector-specific guidelines, Code of practice for information security controls based on ISO/IEC 27002 for cloud services

STUDENT NOTES

- ISO/IEC 27018 Standard describing sector-specific guidelines, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27701:2019 An extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management

 Requirements and guidelines
- ISO 27799 Standard describing sector-specific guidelines, Information security management in health using ISO/IEC 27002.

ISO 27000: FUNDAMENTALS & VOCABULARY

Earlier in these notes we looked at a range of common management system terms and definitions that are taken from Annex SL, however ISO 27000 sets out a number of additional ISMS specific terms and definitions. It is important that whenever a term is used in conjunction with the ISO 27000 series, that we use the term in the way that ISO 27000 means it.

The table below sets out the main ISO 27000 terms and definitions that we will be referring to continually throughout this course.

TERM	DEFINITION			
Availability	Property of being accessible and usable on demand by an authorized entity			
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes			
Event	Occurrence or change of a particular set of circumstance			
Information Security	y Preservation of confidentiality, integrity and availability of information			
Information Security EventIdentified occurrence of a system, service or network state indicating a post breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant				
Information Security Incident Single or a series of unwanted or unexpected information security events that h significant probability of compromising business operations and threatening information security				
Information Security	Set of processes for detecting, reporting, assessing, responding to, dealing with, and			
Incident Management	learning from information security incidents			
Information System	Set of applications, services, information technology assets, or other information- handling components			
Integrity	Property of accuracy and completeness			
Level of Risk	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood			
Risk Acceptance	Informed decision to take a particular risk			
Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk			
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation			

STUDENT NOTES

TERM	DEFINITION	
Risk Criteria	Terms of reference against which the significance of risk is evaluated	
Pick Evaluation	Process of comparing the results of risk analysis with risk criteria to determine	
	whether the risk and/or its magnitude is acceptable or tolerable	
Risk Identification	Process of finding, recognizing and describing risks	
Risk Owner	Person or entity with the accountability and authority to manage a risk	
Risk Treatment	Process to modify risk	
Throat	Potential cause of an unwanted incident, which can result in harm to a system or	
illeat	organization	
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats	

STUDENT NOTES

ISO 27001 CLAUSE STRUCTURE AND PRINCIPLES

The ISO 27001 standard follows the Annex SL format, which means its main clauses are:

- 1. Scope
- 2. Normative references
- 3. Terms and definitions
- 4. Context of the organization
- 5. Leadership
- 6. Planning
- 7. Support
- 8. Operation
- 9. Performance evaluation
- 10. Improvement

The structure of the standard is completed by Annex A, a normative Annex containing reference control objectives and controls (see more information below).

DETERMINING THE SCOPE OF THE MANAGEMENT SYSTEM

The scope defines where and for what exactly the ISMS is applicable and where and for what it is not. Establishing the scope is therefore a key activity that determines the necessary foundation for all other activities in the implementation of the ISMS. For instance, risk assessment and risk treatment, including the determination of controls, will not produce valid results without having a precise understanding of where exactly the ISMS is applicable. Precise knowledge of the boundaries and applicability of the ISMS and the interfaces and dependencies between the organization and other organizations is critical as well.

The following factors can affect the determination of the scope:

- the external and internal issues of the organization
- the interested parties and their requirements
- the readiness of the business activities to be included as part of ISMS coverage
- all support functions, i.e. functions that are necessary to support these business activities (e.g. human resources management; IT services and software applications; facility management of buildings, physical zones, essential services and utilities) and
- all functions that are outsourced either to other parts within the organization or to independent suppliers.

STUDENT NOTES

The scope of an ISMS can be very different from one implementation to another. For instance, the scope can include:

- one or more specific processes
- one or more specific functions
- one or more specific services
- one or more specific sections or locations
- an entire legal entity
- an entire administrative entity and one or more of its suppliers.

Attention should be given to the interdependencies between different functions and processes. For example, if the scope is restricted to the Production process of the organization (e.g. production of metallic frames), the organization should take into consideration that in order for this process to operate, other department's activities are needed (e.g. IT, HR, Management, Procurement etc).

Documented Information

ISO 27001 requires that an organization maintains documentation appropriate to the needs of itsmanagement system but it does not define any specific mandatory procedures (in their typical format).

Records and Documents

There are numerous areas within ISO 27001 where there is a mandatory requirement to produce and retain records. Mandatory documents required by ISO 27001:

- Scope of the ISMS (clause 4.3)
- Information security policy and objectives (clauses 5.2 and 6.2)
- Risk assessment and risk treatment methodology (clause 6.1.2)
- Statement of Applicability (clause 6.1.3 d)
- Risk treatment plan (clauses 6.1.3 e and 6.2)
- Risk assessment report (clause 8.2)
- Definition of security roles and responsibilities (controls A.7.1.2 and A.13.2.4*)
- Inventory of assets (controls A.8.1.1*)
- Acceptable use of assets (control A.8.1.3*)
- Access control policy (control A.9.1.1*)
- Operating procedures for IT management (control A.12.1.1*)
- Secure system engineering principles (control A.14.2.5*)
- Supplier security policy (control A.15.1.1*)
- Incident management procedure (control A.16.1.5*)
- Business continuity procedures (control A.17.1.2*)
- Statutory, regulatory, and contractual requirements (control A.18.1.1*)

STUDENT NOTES

Mandatory records required by ISO 27001:

- Records of training, skills, experience and qualifications (clause 7.2)
- Monitoring and measurement results (clause 9.1)
- Internal audit programme (clause 9.2)
- Results of internal audits (clause 9.2)
- Results of the management review (clause 9.3)
- Results of corrective actions (clause 10.1)

* Documentation requirements of the Annex A (controls) are only applicable if the organization has selected to include the specific control in its implementation. For more information about inclusion and exclusion of controls please refer to par. Risk Based thinking and Annex A below.

Benefits of documentation

There are clear benefits of documenting critical aspects of the system. For example:

- Reduced risk that knowledge leaves with the job holder
- Documents can be used as training aids
- Clarity of communications
- Consistency of work methods
- Records demonstrate facts and history and can be used to demonstrate conformity
- Records and data can be reliably fed into the management review process.

Documented Information - Definition and Context

A management system will need a proportion of documented information to enable it to consistently control certain (but possibly not all) activities. *Documented Information* is defined in Annex SL as:

"Information required to be controlled and maintained by an organisation and the medium on which it is contained"

The definition is appended by some guidance notes that add context to the overall definition. They are:

- Note 1: Documented information can be in any format and media, and from any source
- Note 2: Documented information can refer to:
 - Solution The management system and related processes
 - Information created in order for the organisation to operate (documentation)
 - Service of the results achieved

These notes therefore clarify the "documentation" includes both documents (that contain information which may change and therefore require change control) and records (statements of fact that should not change, but should be protected). Note 1 also indicates that "document" could include hard copy printed documents, soft copy electronic documents, photographic instructions, video clip procedures etc.

STUDENT NOTES

The general auditing principle of "open mindedness" is important when assessing documentation. Not all systems may be developed using "traditional" formats and structures.

Documented Information – Requirements

The requirement for documented information within the Annex SL format is broken down into three disciplines:

- General
- Creating and Updating
- Control

Documented Information - General

Documented information is needed to define and communicate information security objectives, policy, guidelines, instructions, controls, processes, procedures, and what persons or groups of people are expected to do and how they are expected to behave. Documented information is also needed for audits of the ISMS and to maintain a stable ISMS when persons in key roles change. Further, documented information is needed for recording actions, decisions and outcome(s) of ISMS processes and information security controls.

Documented information can contain:

- information about information security objectives, risks, requirements and standards;
- information about processes and procedures to be followed; and
- records of the input (e.g. for management reviews) and the outcomes of processes (including plans and outcomes of operational activities).

There are many activities within the ISMS that produce documented information that is used, most of the time, as an input for another activity. ISO/IEC 27001 requires a set of mandatory documented information and contains a general requirement that additional documented information is required if it is necessary for the effectiveness of the ISMS. The amount of documented information needed is often related to the size of the organization. In total, the mandatory and additional documented information contains sufficient information to allow the performance evaluation requirements to be carried out.

Documented Information - Creating and Updating

The organization identifies in detail how the documented information is best structured and defines a suitable documentation approach. Review and approval by appropriate management ensures that the documented information is correct, suitable for the purpose, and in an adequate form and detail for the intended audience. Regular reviews ensure continued suitability and adequacy of documented information.

Documented information may be retained in any form, e.g. traditional documents (in both paper and electronic form), web pages, databases, computer logs, computer generated reports, audio and video. Moreover,

documented information may consist of specifications of intent (e.g. the information security policy) or records of performance (e.g. the results of an audit) or a mixture of both.

STUDENT NOTES

Control of Documented Information

The organization manages documented information throughout its lifecycle and makes it available where and when needed.

Once approved, the documented information is communicated to its intended audience. Documented information is available where and when it is needed, while preserving its integrity, confidentiality, and relevance throughout the whole lifecycle.

The general disciplines and control requirements remain as follows;

- Availability
- Protection
- Distribution, access and retrieval
- Storage and protection
- Change control (appropriate to documents but NOT records)
- Retention and disposal
- Control of documents of external origin (e.g. drawings or a recipe from a customer, manufacturer's user manuals, technical specifications etc)

RISK BASED THINKING

ISO 27001 raises the visibility of the concept of "risk-based thinking" as an input into the development and improvement of system controls. It identifies that some form of analysis will be required in order for appropriate risk control measures (preventative actions) to be identified and developed.

Annex SL defines "risk" as;

"Effect of uncertainty" (from Annex SL Appendix 2, 3.9)

However, that short definition is accompanied by some explanatory notes to add context. Note 1 states that; *"An effect is a deviation from the expected – positive or negative"*

Thus, introducing the concept of "upside risk" – a circumstance where things turn out better than expected. Note 2 states that;

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

This emphasizes the fact that not everything is known or even knowable, and a robust management system is therefore one that accepts that and identifies what controls may be prudent in terms of contingency. Note 3 states that;

"Risk is often characterized by reference to potential "events" and "consequences" or a combination of these"

STUDENT NOTES

While note 4 states that;

"Risk is often expressed in terms of a combination of the consequences of an event and the associated "likelihood" of occurrences"

The structure of ISO 27001 subdivides risks into two categories during planning:

- risks and opportunities relevant to the intended outcome(s) of the ISMS as a whole; and
- information security risks that relate to the loss of confidentiality, integrity and availability of information within the scope of the ISMS.

Risks that fall into the first category can be risks relating to the ISMS itself, the ISMS scope definition, top management's commitment to information security, resources for operating the ISMS, etc. Opportunities that fall into this category can be opportunities relating to the outcome(s) of the ISMS, the commercial value of an ISMS, the efficiency of operating ISMS processes and information security controls, etc.

The second category consists of all risks that directly relate to the loss of confidentiality, integrity and availability of information within the scope of the ISMS. These risks should be handled in accordance with information security risk assessment and information security risk treatment.

Information security risk assessment

The organization defines an information security risk assessment process that:

- establishes and maintains:
 - ⇒ the risk acceptance criteria; and
 - criteria for performing information security risk assessments, which can include criteria for assessing the consequence and likelihood, and rules for the determination of the level of risk; and
- ensures that repeated information security risk assessments produce consistent, valid and comparable results.

The information security risk assessment process is then defined along the following sub-processes:

- identification of information security risks:
 - identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS; and
 - ➡ identify the risk owners associated with these risks, i.e. identify and appoint persons with the appropriate authority and responsibility for managing identified risks.
- analysis of the information security risks:
 - assess the potential consequences in case the identified risks materialize, e.g. direct business impacts such as monetary loss or indirect business impacts such as damage in reputation. Assessed consequences can be reported with quantitative or qualitative values;
 - assess the realistic likelihood of occurrence of the identified risks, with quantitative (i.e. probability or frequency) or qualitative values; and
 - ➡ determine the levels of identified risk as a predefined combination of assessed consequences and assessed likelihoods; and

STUDENT NOTES

- evaluation of the information security risks:
 - ⇒ compare the results of risk analysis with the risk acceptance criteria established before; and
 - prioritize the analysed risks for risk treatment, i.e. determine urgency of treatment for risks that are considered as unacceptable, and sequence if several risks need treatment.

The information security risk assessment process is then applied.

All steps of the information security risk assessment process as well as the results of its application are retained by the organization as documented information.

Information security risk treatment

Information security risk treatment is the overall process of selecting risk treatment options, determining appropriate controls to implement such options, formulating a risk treatment plan and obtaining approval of the risk treatment plan by the risk owner(s).

Steps of the information security risk treatment process:

- select appropriate information security risk treatment options, taking account of the risk assessment results;
- determine all controls that are necessary to implement the information security risk treatment option(s) chosen;
- compare the controls with those in Annex A and verify that no necessary controls have been omitted;
- produce a Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;
- formulate an information security risk treatment plan; and
- obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

All steps of the information security risk treatment process as well as the results of its application are retained by the organization as documented information.

STUDENT NOTES

Annex A

ISO 27001, Annex A contains a comprehensive list control. Not every control withinISO 27001, Annex A needs to be included. Any control within ISO/IEC 27001, Annex A that does not contribute to modifying risk should be excluded and justification for the exclusion should be given.

The Annex A is structured in chapters containing several controls. For each of these chapters at least one control is proposed that has the ability to treat (to an extend) the relevant objective.

The following figure shows the different categories and their corresponding number. The categories range from numbers 5 to 8. Typically, any reference to an Annex A component, starts with the letter A. (e.g. A.5.1).



Annex A (normative)

Information security controls reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022^[1], Clauses 5 to 8, and shall be used in context with 6.1.3.

Table A.1 — Information security controls

5	Organizational controls		
5.1	Policies for information secu- rity	Control Information security policy and topic-specific policies shall be de- fined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	
5.2	Information security roles and responsibilities	Control Information security roles and responsibilities shall be defined and allocated according to the organization needs.	
5.3	Segregation of duties	Control Conflicting duties and conflicting areas of responsibility shall be seg- regated.	
5.4	Management responsibilities	Control Management shall require all personnel to apply information security in accordance with the established information security policy, top- ic-specific policies and procedures of the organization.	

STUDENT NOTES

Statement of Applicability (SoA)

The SoA contains:

- all necessary controls (as determined in 6.1.3 b) and 6.1.3 c)) and, for each control:
 - the justification for the control's inclusion; and
 - ⇒ whether the control is implemented or not (e.g. fully implemented, in progress, not yet started);
- the justification for excluding any of the controls in ISO/IEC 27001, Annex A.

Justification for including a control in part relies on the effect of the control in modifying an information security risk. A reference to information security risk assessment results and the information security risk treatment plan should be sufficient, along with the information security risk modification expected by the implementation of necessary controls

Justification for excluding a control contained within ISO/IEC 27001, Annex A can include the following:

- it has been determined that the control is not necessary to implement the chosen information security risk treatment option(s);
- the control is not applicable because it is outside the scope of the ISMS (e.g. ISO/IEC 27001, A.8.30 Outsourced development is not applicable if all the organization's system development is performed inhouse); and
- it is obviated by a custom control (e.g. in ISO/IEC 27001:2022, A.8.12 management of data leakage prevention couldbe excluded if a custom control prevents the data leakage).

An organization may use national and international standards as source(s) of control set for controls that are determined as necessary in the organization's Statement of Applicability. (e.g. controls related to cloud security can be retrieved from ISO 27017).

STUDENT NOTES

ISO 27002

ISO 27002 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This International Standard is designed to be used by organizations that intend to:

- select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
- implement commonly accepted information security controls;
- develop their own information security management guidelines;

ISO 27002 contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls.

Each clause defining security controls contains one or more main security categories. The order of the clauses in this standard does not imply their importance. Depending on the circumstances, security controls from any or all clauses could be important, therefore each organization applying this standard should identify applicable controls, how important these are and their application to individual business processes. Furthermore, lists in this standard are not in priority order.

Each main security control category contains:

- a control objective stating what is to be achieved;
- one or more controls that can be applied to achieve the control objective.

Control descriptions are structured as follows:

🌭 Control

Defines the specific control statement, to satisfy the control objective.

Solution Sector Secto

Provides more detailed information to support the implementation of the control and meeting the control objective. The guidance may not be entirely suitable or sufficient in all situations and may not fulfil the organization's specific control requirements.

Other information

Provides further information that may need to be considered, for example legal considerations and references to other standards. If there is no other information to be provided this part is not shown.

As an example, below is described 5.1 Management direction for information security:

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

STUDENT NOTES

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives. Information security policies should address requirements created by:

- business strategy;
- regulations, legislation and contracts;
- the current and projected information security threat environment.

The information security policy should contain statements concerning:

- definition of information security, objectives and principles to guide all activities relating to information security;
- assignment of general and specific responsibilities for information security management to defined roles;
- processes for handling deviations and exceptions.

At a lower level, the information security policy should be supported by topic-specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics.

Examples of such policy topics include:

- access control (see Clause 9);
- information classification (and handling) (see 8.2);
- physical and environmental security (see Clause 11);
- end-user oriented topics such as:
 - ⇒ acceptable use of assets (see 8.1.3);
 - ⇒ clear desk and clear screen (see 11.2.9);
 - ⇒ information transfer (see 13.2.1);
 - ⇒ mobile devices and teleworking (see 6.2);
 - ⇒ restrictions on software installations and use (see 12.6.2);
- backup (see 12.3);
- information transfer (see 13.2);
- protection from malware (see 12.2);
- management of technical vulnerabilities (see 12.6.1);
- cryptographic controls (see Clause 10);
- communications security (see Clause 13);
- privacy and protection of personally identifiable information (see 18.1.4);
- supplier relationships (see Clause 15).

These policies should be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an "information security awareness, education and training programme" (see 7.2.2).

STUDENT NOTES

Other information

The need for internal policies for information security varies across organizations. Internal policies are especially useful in larger and more complex organizations where those defining and approving the expected levels of control are segregated from those implementing the controls or in situations where a policy applies to many different people or functions in the organization. Policies for information security can be issued in a single "information security policy" document or as a set of individual but related documents.

If any of the information security policies are distributed outside the organization, care should be taken not to disclose confidential information. Some organizations use other terms for these policy documents, such as "Standards", "Directives" or "Rules".

ର REVISION HINTS ରହ

- Scould you explain the purpose and potential benefits of a documented ISMS?
- Scould you explain the structure of a typical ISMS?
- Scould you explain why it is only **documents** and not **records** that require version control?
- Could you identify the basic functions of an ISMS and explain the potential benefits of implementing an ISMS?
- Scould you describe the difference between ISO 27000, ISO 27001 and ISO 27002?
- Scould you explain what the purpose of the Statement of Applicability?

STUDENT NOTES

ISO 19011 GUIDELINES FOR AUDITING MANAGEMENT SYSTEMS

ISO 19011:2018 (Guidelines for Auditing Management Systems) is the third edition of an International Standard designed to provide guidance on auditing Management Systems, including the principles of auditing, managing an audit program and conducting Management Systems audits. Furthermore, the standard includes guidance on the evaluation of competence of individuals involved in audit process and specifically people who managing the audit program, auditors and audit teams. As is a guidance document it is not used as auditable or certification standard.

The most significant changes incorporated into ISO 19011:2018 compared to the previous version are:

- addition of a new seventh audit principal Risk-based approach to audit
- expansion of the guidance on managing an audit program, including the audit program risk
- expansion of the guidance on conducting an audit, particularly in respect of audit planning
- expansion of the generic competence requirements for auditors
- focus on processes and not just outputs as audit planning instead of audit plan, audit reporting instead of audit report etc.
- removal of previous version's annex A which illustrated guidance and examples of discipline specific knowledge and skills of auditors, (due to the large numbers of individual Management System standards, it was not practical competence requirements for all disciplines to be included)
- expansion of previous version's annex B and now as ISO 19011: 2018 annex A to include guidance on a range
 of new concepts including but not limited to, auditing context, auditing leadership and commitment, auditing
 risks and opportunities, supply chain audit, virtual audits and auditing compliance.

This Auditor / Lead Auditor course is designed to develop the students' competencies, according to standard ISO 19011 as well as ISO/IEC 17021-1.

ISO 19011 clarifies that its guidance is focused on internal audits (first party) and external audits by interested parties (second party) as well as it can be useful for external audits (third party) by Certification Bodies conducted for statutory, regulatory and similar purposes. Especially for accredited Certification Bodies and certification audits (third party) the appropriate standard is ISO/IEC 17021-1 which contains requirements for Certification Bodies providing audit and certification of all types Management Systems. In this case, ISO 19011 can only be used as a supplementary document for any Certification Body which wishes to develop its own audit process. ISO 19011 is a **guidance** document.

STUDENT NOTES

TERMS AND DEFINITIONS

For the purpose of ISO 19011, a number of audit terms and definitions apply. The table below depicts the main ISO 19011 terms and definitions.

TERM	DEFINITION			
Audit	Systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled			
Audit Criteria	Set of requirements used as reference against which objective evidence is compared (Requirements may include policies, procedures, work instructions, legal requirements, contractual obligations etc.)			
Audit Findings	Results of the evaluation of the collected audit evidence against the audit criteria (Audit findings indicate conformity or nonconformity)			
Audit Conclusion	Outcome of the audit, after consideration of the audit objectives and all audit findings			
Audit Client	Organization or person requesting an audit			
Auditee	Organization as a whole or parts thereof being audited			
Auditor	Person who conducts an audit			
Audit team	One or more auditors conducting an audit, supported if needed by technical experts			
Technical Expert	Person who provides specific knowledge or expertise to the audit team			
Audit Programme	Arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose			
Audit Plan	Description of the activities and arrangements for an audit			
Audit Scope	Extent and boundaries of an audit			
Ethical Conduct	The foundation of professionalism. Trust, integrity, confidentiality and discretion			
Integrity	The foundation of professionalism			
Fair Presentation	The obligation to report truthfully and accurately. Significant obstacles encountered during the audit and unresolved diverging opinions between the audit team and auditee are reported			
Due Professional Care	The application of diligence and judgement in auditing			
Confidentiality	Security of information.			
Independence	The basis for the impartiality of the audit and objectivity of audit conclusions			

STUDENT NOTES

TERM	DEFINITION
Evidence Based Approach	The rational method for reaching reliable and reproducible audit conclusions in a systematic audit process. It is based on samples of information available, since an audit is conducted during a finite period of time and with finite resources. The appropriate use of sampling is closely related to the confidence that can be placed in audit conclusions
Risk-based approach	An audit approach that considers risks and opportunities. The risks and opportunities must substantively 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 audit programme objectives
First Party Audit	Internal audit is conducted by, or on behalf of, the organization itself
Second Party Audit	External Audit is conducted by parties having an interest in the organization, such as customers, or other individuals on their behalf
Third Party Audit	External audit is conducted by external, independent auditing organizations, such as those providing certification/registration of conformity to specific certification standard's requirements or governmental agencies

During the audit, the auditors must perform their work ethically, with honesty and responsibility. Their findings, audit conclusions and audits reports must reflect truthfully and accurately the audit activities. Furthermore, the auditors must have the ability to make reasoned judgments in all audits situation and must remain objective throughout the audit process. Their working methods must be transparent and, where necessary, explained to the auditee. Otherwise, confusion and suspicion will be created to the auditee. It is not good practice, if the auditee considers that the auditor's job is unknown and inaccessible to him or her.

During this course, the students will be familiarized with these definitions and exploring the context of each, so will have a clear understanding of how these terms are applied in relation to first, second and third party audits.

FIRST PARTY AUDITS (INTERNAL AUDITS)

«Internal audits are conducted by, or on behalf of, organization itself and their results are one of Management review inputs. The audit conclusions are used to evaluate the effective implementation and maintenance of Management System and simultaneously are the basis for the evaluation of Management System's conformity with the organization's own requirements as well as the certification standards' requirements».

A first party (internal) audit process may differ quite considerably to the process followed during a second and third party audit due to its nature. The people involved (auditors and auditees) are generally more familiar between them, the scope, the objectives and audit criteria are usually known to them so a formal opening meeting is not always necessary. However, the internal audits need to conform with the audit principles outlined in ISO 19011, especially with regard to managing an audit program, conducting an audit as well as competence and impartiality of internal auditors.

STUDENT NOTES

SECOND PARTY AUDITS (EXTERNAL AUDITS)

«Audits which are conducted by parties having an interest in the organization, such as customers, or other individuals / impartial Bodies – Organizations on their behalf».

The most common type of second party audit is an audit by a customer on a supplier and its aim is usually to determine the quality level of the products and services provided to the customer or to compare the quality level of different customer's suppliers. If the audit results are very unfavorable then the customer may terminate the contract. Generally speaking, the consequences of a poor result of a second party audit are usually more severe that on first or third party audit.

THIRD PARTY AUDITS (EXTERNAL AUDITS)

«Audits which are conducted by external, independent auditing organizations, such as those providing certification/registration of conformity to specific certification standard's requirements or governmental agencies». In recent years, the interest and the demand for third party audits has increased considerably. An Organization which implements an effective Management System wants to demonstrate its ability to consistently provide products and services that meet or exceed its customers' requirements. For that reason, it requests an accredited Certification Body to evaluate its Management System's performance according to specific criteria. In case of positive results, the Certification Body can award the Organization with a certificate of conformity and enhance the confidence and trust of its customers about its effective operation. The certification is awarded and is maintained through a program of third-party audits. The independence, impartiality and competence of a Certification Body are assured of accreditation by National Accreditation Body.

The Certification Body's accreditation and independence create additional confidence in the integrity of certification process and in the added value of certification. ISO 19011 requires greater independence of third-party auditors than the first party ones. For that reason, in the new version of standard ISO 19011 and in the principal «Independence» is written exactly: «For internal audits, auditors should be independent from the function being audited, **if practicable**». On the contrary, Accredited Certification Bodies require their auditors to declare in advance any potential conflict of interest with the Organizations that they have been assigned to audit.

STUDENT NOTES

ର REVISION HINTS ରହ

- Scan you describe the purpose of ISO 19011 and how it is used?
- Scan you describe the difference between first, second and third party audit?
- Can you describe the role of each of them in context of an audit?
 - Audit Client?
 - Auditor?
 - Auditee?
 - Technical Expert?
- Scan you explain the term «audit scope» and describe why the scope must be clearly defined?
- Can you explain the term «audit criteria» and give some examples of typical criteria that would be used during first, second and third party audit?

STUDENT NOTES

DIFFERENT TYPES OF AUDIT, DIFFERENT TYPES OF APPROACH

WHAT IS AN AUDIT?

Audits are conducted for lots of different reasons so there are lots of different types of audit. They vary in extent and boundaries, in complexity and in focus.

Each audit has its own parameters. Each of these parameters has its own definition which is outlined in ISO 19011.

The main parameters are listed below:

- What are the extent and the boundaries of audit? («audit scope»)
- What the audit will check against? («audit criteria»)
- What is the reason for conduct of audit? («audit objectives»)

These parameters must be clearly understood by both auditor and auditee. An audit is a process designed to promote clarity and transparency. The opposite situation creates confusion, suspicion and stress to the auditee.

DIFFERENT AUDIT TYPES

Conformance audits

There are some Organization's activities as heavily automated processes or many medical processes etc. which are supported by detailed procedures and instructions. This documentation must explicitly be followed in order important results to be achieved by the processes. On the other hand, methods may or may not be so critical. In the case where the results as well as the methods are important, the auditor will have to adopt a conformance approach and will have to clarify whether these results have been achieved.

Effectiveness audits

Sometimes the methods are not so critical. Some activities and some processes such as Sales, Marketing, Customer Services and Training may actually require flexibility in order to achieve their best results. A good auditor must have the ability to adopt his or her audit and to understand that in some cases, differences in methods do not present significant risks and problems. In fact, it is better for the process to be flexible than not to. When the working methods are flexible and not crucial then the auditor will have to adopt an effectiveness approach and will have to clarify whether the process' measured indexes have achieved their targets.

STUDENT NOTES

Compliance audits

The term «compliance» is reserved for audits where the criteria contain mandatory requirements, mostly legal requirements. In compliance audits there is no flexibility and an increased requirement that the auditor very clearly understands the requirements and interprets them correctly, as the potential impact can have a significant implication for the auditee.

Improvement audits

Sometimes the primary focus of the audit is to establish whether situations have been improved at different times. This is a «follow up» audit and is scheduled in a future time than a previous conformance and/or effectiveness and/or compliance audit which conducted in a past time and identified problems. The aim of the «follow up» audit is to establish that problems have been resolved and/or situations have been improved. In order for the auditor to focus accurately on the audit objectives it is important that in planning the audit, the auditor does some background research to establish the levels of past performance in order to clearly and accurately report the «before» and «after» situation. This generally involves examining previous audit results and process performance indicators in advance of performing the audit.

Procedural audits

A procedural audit will generally be quite narrow in scope and will look in detail at the execution of a particular operation. Good procedural audits don't just examine in detail whether the procedure is being followed, but also if the procedure is effective. It is not satisfactory that employees simply follow the procedure. If the procedure is not updated or has major omissions, it might be better if the employees do not follow it. Procedural audits are useful at getting detailed information about conformity, but usually limited to a single task or activity. Many internal (first party) audits will be procedural audits but a good audit process will not be made exclusively of them.

Process audits

What are process audits?

See below some useful ISO 9000 definitions:

«Specified way to carry out an activity or a process» ISO 9000 definition of a <u>procedure (</u>3.4.5)

«A set of inter-related activities that transforms inputs into outputs» ISO 9000 definition of a <u>process</u> (3.4.1)

STUDENT NOTES

The key word that distinguishes the two terms is **«inter-related»**. A process is a **collection of activities**, from end to end, that transforms the process input into its output. The scope of the process audit is usually quite broader than the one of the procedural audit:



As a general rule, a **procedural audit** will have a very narrow scope and will focus on **conformity**, whereas a **process audit** (as it takes in various interfaces and inter-relationships) will focus more on **process' efficiency**.

A process audit looks at the big picture, and is therefore a much bigger and complicated work. It is complex. Process audits examine the efficiency of the operation. Why is efficiency important? Because given infinite resources and time, anyone can deliver conformity but the aim is to achieve efficiency at an acceptable product's or service's price. Otherwise, the customer will look for the product or service to competitors.

Looking at the above from an information security perspective, if given infinite resources and time, anyone can create a very secure system (not 100% secure but pretty close), but the aim is to achieve the right amount of security needed by the organization allowing for the necessary amount of functionality. Otherwise, the organization will have huge barriers in its operation and have difficulties satisfying the various stakeholders.

So, in an ISO 27001 audit of an ISMS, it is desirable for the auditor to ascertain that what the organization needs regarding information security are identified and suitable controls are designed and implemented effectively.

PLANNING A PROCESS AUDIT

Because process audits are a substantial task and can be quite complex, planning is important. There will not normally be a convenient internal document that defines how the auditor should conduct a process audit in any Organization. The auditor must plan his/her activities, using in each case the Organization's documentation and context. This will involve requesting relevant policies, Organization charts, procedures and process maps that may exist so that the auditor can draw up his/her checklist from an informed perspective, using the below diagram.



STUDENT NOTES

ର REVISION HINTS ରହ

In context of an audit:

- Scan you explain the meaning of audit scope, objectives and criteria?
- Scan you explain why it is crucial the above terms to be crystal clear during an audit?
- Scan you explain the difference between conformance and compliance?
- Scan you explain the difference between conformance and effectiveness?
- Scan you explain the difference between a procedural approach and a process approach?
- Scan you describe the strengths and limitation of each approach?

STUDENT NOTES

KEY ISSUES INTRODUCED WHEN ISO 27001 ADOPTED THE ANNEX SL FORMAT

ISO 27001 is the first issue of ISO 27001 that adopts the Annex SL common management system format. The adoption of that format has introduced some significant considerations for auditors, as it adjusted the focus on several issues (such as "documentation" and "risk") and it raised the status and importance of issues such as Top Management Commitment, the overall Effectiveness of the system and the identification of Internal and External Issues.

CONTEXT AND SCOPE

One of the key themes that has emerged as a result of the adoption of the Annex SL format has been the issue of "Organisational Context". Not all organisations are the same, and it follows that not all management systems will be the same. Context is an issue as much for auditors of a management system as it is for those that develop and manage management systems. Controls must be appropriate, proportionate and effective. What works for one organisation may be wholly inappropriate for another. It is unlikely that, if an organisation in developing its system has adopted generic procedures, that the specific context has been fully considered.

Context considerations for employers of auditors

Organisations employing auditors (third party certification bodies, for instance) must consider "context" when allocating an auditor to an audit client.

Questions like:

- Does the auditor have the appropriate sector knowledge to be able to appreciate context?
- Would the auditor be able to take a reliable value judgement on the appropriateness of controls specific to the context?
- Does the auditor have the appropriate technical skills to be able to effectively implement the audit? are created and need to be effectively addressed.

The fact that any given auditor is not able to audit effectively in any given context is not a weakness on anybody's part, it is purely a reflection on that auditor's experience and background in a given sector. It follows that, if an auditor has little or no exposure to a particular type of organisational context, the auditor is probably going to struggle to reliably audit the appropriateness and effectiveness of the controls. An auditor that has specialised throughout his/her professional life in the retail and IT services sector, for example, is unlikely to be able to fully appreciate the context of a telecommunication's provider, at least not without the assistance of a sector specialist. The same applies also for the reverse situation especially for organizations with complex legal and regulatory environment, where the audit criteria are enriched based on these external requirements.

At the same time, an auditor having technical knowledge and experience in specific technologies, may need the assistance of a technology specialist to conduct the audit effectively.

STUDENT NOTES

The consequences of a failure of an auditor to appreciate context could include:

- A superficial audit
- Unreliable and/or inappropriate findings
- Friction and frustration
- A loss of credibility for both auditor and the certification body

Context considerations for certified organisations

Annex SL (Appendix 2) suggests that, as a minimum, in order to fully appreciate the context of the organisation and the appropriateness of the system controls, it should understand:

- The interested parties, internal and external (examples listed earlier) and;
- The requirements of those interested parties;

Some customers have a very low risk acceptance level, others don't. Some sectors have a high level of regulation, others don't. Some suppliers need close and careful management, others don't. Some tasks are highly complex and are difficult to control in the absence of a written procedure, others are not. It is important for an organisation to understand the circumstances that apply so that it may act accordingly.

The consequences of a failure to understand context can include:

- Heavy handed and overly cumbersome procedures (taking a hammer to crack a nut).
- The absence of appropriate controls.
- Procedures that do not effectively control the risks of the process.
- Bureaucratic procedures that burden the organization without reason.
- An inconsistent level of information security within the organization.

In other words, doing too much, doing too little or doing things in a totally inappropriate way.

Determining the Scope of the Management System

Defining the scope of the management system is significant for a number of reasons, particularly when it comes to third party certification. The scope describes the boundaries and limits of the management system and, consequently the certified entity. This is important because it is common for an organisation to seek certification only for a particular function of its operation, or for a single site. Certification is often used to help the organisation secure contracts, and an organisation may only need a part to be certified for that purpose.

It is important to understand that whatever scope is defined by the organisation within its own management system, will also be specified on the certificate. This helps prospective customers understand the limits of the certification and prevents the organisation making false representation by claiming certification for parts of the organisation that are not certified. Excluding parts of the organisation from scope is in no way a dodge, as the scope that is stated on the certificate will not include the excluded parts. The customer will then be able to make an informed decision as to whether the certification the organisation holds is broad enough for its purposes.

STUDENT NOTES

ISO 27006 mandates, that in order to provide the required transparency to the audience of the certificate, the version of the statement of applicability is included in the certification documents. This means that the certificate is defined also by another dimension – that of controls being implemented. The parameters regarding scope are mentioned also above.

Internal & External Issues

Annex SL (Appendix 1) identifies that management systems adopting the Annex SL format need to pay greater attention to identifying and understanding internal and external issues. This is an important part of defining the context of the management system.

Specifically, an organisation should carefully analyse its internal and external interfaces and identify the internal and external interested parties, which will in turn help it to identify their needs and expectations and develop controls appropriately.

Annex SL (Appendix 1) identifies a number of examples that could be considered:

- Organizations (of various types and sizes): the decision-makers within an organization who approve work to implement and achieve conformance to the MSS;
- Customers/end-users, i.e. individuals or parties that pay for or use a product (including service) from an organization;
- Supplier organizations, e.g. producer, distributor, retailer or vendor of a product, or a provider of a service or information;
- Management system service (MSS) provider, e.g. MSS certification bodies, accreditation bodies or consultants;
- Regulatory bodies;
- Non-governmental organizations

Obviously, this list is neither exhaustive nor generic, but it offers guidance on the general principle that key internal and external interfaces need to be identified, understood and managed. It is not suggested that each interface or interested party is of equal importance, and an organisation, in understanding the interface must consider the most appropriate and efficient way of managing that interface, appropriate to (among other things) its significance.

ISO 27003, provides a more customized guidance regarding context of an Information security management system.

More specifically, ISO 27003 on the subject of an ISMS context, the analysis of context is concerned with external and internal issues that in some way affect information security and how information security can be managed, and that are relevant to the organization's objectives.

STUDENT NOTES

External issues are those outside of the organization's control. This is often referred to as the organization's environment. Analysing this environment can include the following aspects:

- a) social and cultural;
- b) political, legal, normative and regulatory;
- c) financial and macroeconomic;
- d) technological;
- e) natural; and
- f) competitive.

These aspects of the organization's environment continually present issues that affect information security and how information security can be managed. The relevant external issues depend on the organization's specific priorities and situation.

For example, external issues for a specific organization can include:

- g) the legal implications of using an outsourced IT service (legal aspect);
- h) characteristics of the nature in terms of possibility of disasters such as fire, flood and earthquakes (natural aspect);
- i) technical advances of hacking tools and use of cryptography (technological aspect); and
- j) the general demand for the organization's services (social, cultural or financial aspects).

Internal issues are subject to the organization's control. Analysing the internal issues can include the following aspects:

- k) the organization's culture;
- I) policies, objectives, and the strategies to achieve them;
- m) governance, organizational structure, roles and responsibilities;
- n) standards, guidelines and models adopted by the organization;
- contractual relationships that can directly affect the organization's processes included in the scope of the ISMS;
- p) processes and procedures;
- **q**) the capabilities, in terms of resources and knowledge (e.g. capital, time, persons, processes, systems and technologies);
- r) physical infrastructure and environment;
- s) information systems, information flows and decision-making processes (both formal and informal); and
- t) previous audits and previous risk assessment results.

LEADERSHIP

The actions of top management are important. They are the decision makers, role models, enforcers and also the financial supporters of the management system. Without an effective leadership function, the management system will be adversely affected in a number of crucial ways.

In fact, whilst there will be some variation in the detailed requirements of the top management function between different management system standards (such as the content of the Policy and its specific communication requirements) the general requirements of top management don't vary significantly from one standard to the next.

STUDENT NOTES

They will always contain the common elements of:

- Leadership and Commitment
 - Establishing Policies and Objectives
 - Ensuring integration and implementation of the system and its processes
 - → Provision of necessary resources
 - Communicating priorities and requirements (including the risk acceptance criteria and the organizations risk tolerance).
 - ⇒ Ensuring organisation outputs/objectives are met
 - Direction and support to personnel
 - Promotion and a commitment to a continual improvement culture
 - ⇒ Support to other levels of management
 - Establishing authorising and communicating the top-level Information Security policy
 - ⇒ Defining roles and responsibilities, reporting structures
 - → Oversight of change management
 - Reviewing the system and allocating effort and resources to its efficient operation

The specific focus of Leadership will vary from one management system standard to another, so each standard will contain some specific variation within the Leadership clause. A QMS (quality) management system standard, for example, will be primarily customer and product focussed, an OHSMS (occupational health and safety) management system standard will be primarily focussed on matters of health and wellbeing of those exposed to the organisation's activities, and an EMS (Environmental Management) will be more focussed on matters relating to the prevention of pollution and in this case an ISMS management system standard will be focused on the security of the information identified by the organization as important.

Risks and Opportunities

As mentioned in the introduction section of this document, risk management is located in the heart of an ISMS. The structure of ISO 27001 subdivides risks into two categories during planning:

- risks and opportunities relevant to the intended outcome(s) of the ISMS as a whole; and
- information security risks that relate to the loss of confidentiality, integrity and availability of information within the scope of the ISMS.

Risks that fall into the first category can be risks relating to the ISMS itself, the ISMS scope definition, top management's commitment to information security, resources for operating the ISMS, etc. Opportunities that fall into this category can be opportunities relating to the outcome(s) of the ISMS, the commercial value of an ISMS, the efficiency of operating ISMS processes and information security controls, etc.

The second category consists of all risks that directly relate to the loss of confidentiality, integrity and availability of information within the scope of the ISMS. These risks should be handled in accordance with information security risk assessment and information security risk treatment.

STUDENT NOTES

Consequently, as an overall requirement, the management system should develop contingency appropriate to the level of uncertainty. Not all management information is knowable, but better and worse case scenarios can often be considered.

The Effect of Uncertainty (Risk) on Planning

Where there is certainty, planning can be precise. Where there is uncertainty, precise planning is not possible. A plan that takes account of uncertainty is said to provide for CONTINGENCY.

Contingency should be proportionate to the level of uncertainty and its effect. That is, if something is unlikely to occur and/or the effect of uncertainty is minor, a lot of contingency (which can be expensive) would be disproportionate. Obviously when an auditor is assessing the appropriateness of the level of contingency, it must be remembered that it is not a precise science. One of the factors an auditor may consider when looking at whether contingency is appropriate (and to what level) is whether the uncertain outcome has ever actually happened previously and, if it has, what were the consequences.

ର REVISION HINTS ର

In context of an audit:

- Sould you explain how the differences in context can affect an ISMS audit?
- Scould you explain the difference between conformance and compliance?
- Sould you explain the difference between conformance and effectiveness?
- Scould you explain the difference between a procedural approach and a process approach and the strengths and limitations of each approach?
- Sound you explain how an auditor may assess whether the organisation has identified its risks and opportunities and its significant Internal and External Issues?
- Scould you explain the two layers of Information Security Risk Management?
- Could you explain what an auditor should keep in mind when reviewing the scope of an ISMS?
- Scould you explain how risk management is involved also in auditing?

STUDENT NOTES

ISO 19011:2018 MANAGING AN AUDIT PROGRAM

MANAGING AN AUDIT PROGRAM

In this section, the important stages of an audit process will be illustrated as outlined in ISO 19011. The standard (ISO 19011) defines the main stages of managing an audit program, whether it is on first, second or third party basis. So, when reading the following sections, please keep in mind that the information provided has a wide audience and some sentences should be altered accordingly to fit third party audits only.

ISO 19011 advises that an audit program must be established to include audits which address one or more Management Systems standards or other audits requirements. Generally speaking, **no audit activity can be excluded from the audit program**. The extent of an audit program will depend on many factors. These include the size and nature of auditee, as well as on the nature, functionality, complexity, the type of risks and opportunities, and the level of maturity of the Management System(s) to be audited.

The design, planning and validation of the audit program requires careful consideration, particularly where an Organization operates in multiple sites and/or where important functions or processes are outsourced and managed by an external provider with related consequences for leadership decisions.

When designing audit programs, it is important to fully address the context of the auditee so the following auditee's information must already be known:

- organizational objectives
- relevant external and internal issues
- the needs and expectations of relevant interested parties
- the risk management process and the risk acceptance criteria
- information security and confidentiality requirements

The information contained within the audit program should now include audit program objectives, scope of each individual audit contained within the program, the audit criteria to be used, audit methods to be employed and the audit type (internal or external). Furthermore, the program must include a schedule showing the number, duration and frequency of planned audits, any risks and opportunities associated with delivering the program, the criteria used for selecting audit team members plus any other relevant documented information.

More emphasis has been placed on monitoring and measuring the implementation of the audit program by suggesting it should be done on an on-going basis to ensure the audit program objectives are being achieved and to identify both the need for changes to the audit program and possible opportunities for improving the program. A clear PDCA structure (Plan – Do – Check – Act) is followed and the specific requirements of ISO 19011 relating to the overall process are detailed in below section.

STUDENT NOTES

Figure 1: Process flow for the management of an audit programme



(From ISO 19011)

STUDENT NOTES

AUTHORITY FOR THE AUDIT PROGRAM

It is important that the audit program is approved and supported by Top Management. There are lots of reasons for this, as example:

- The employees consider the audit important and participate more easily.
- In the cases that the audit team needs recourses to implement the audit program successfully these often be required to be provided by Top Management.
- Any audit barriers and obstacles cab be quickly and easier removed.

ESTABLISHING AN AUDIT PROGRAM

ISO 19011 identifies the following important considerations in establishing audit program. These are listed in details below:

- Establishing audit program objectives which must be consistent with the audit's client strategic direction, as well as supporting their Management System policy and objectives
- Determining and evaluating audit program risks and opportunities which must be communicated to the audit client in order to ensure their accuracy
- Establishing the audit program with the identification of the following:
 - Roles and responsibilities of the individual(s) managing audit program. Among others, the individual has responsibility to communicate the audit program to the audit client and requests its approval.
 - Competence of individual(s) managing audit program. Among the others, the standard advises that individuals may need knowledge of risk management, project and process management and of information and communications technologies, necessary for them to perform their role.
 - ⇒ Establishing extent of audit program that, in specific cases, may consist of a single audit.
 - ⇒ Determining audit program resources.

All the above are important considerations for the development of the audit process. If these aspects are not established at the beginning, the audit process is likely to be inefficient.

IMPLEMENTING AUDIT PROGRAM

Once the audit program has been fully established, it is necessary to move on to the operational planning and management stage. The individuals managing the audit program, among other duties, have the responsibility to communicate the relevant parts of the audit program, including the risks and opportunities involved, to relevant interested parties. ISO 19011 advises that they have to inform periodically those interested parties of the program's progress, using established (external and internal) communications channels.

STUDENT NOTES

ISO 19011 includes the following aspects:

- Defining the objective, scopes and criteria for a single audit which must be consistent with the overall audit program objectives,
- Selecting and determining audit methods, (on-site, remotely or as combination), which must be «suitably balanced» and based on considerations including each method's associated risks and opportunities,
- Selecting audit team members, where the standard recommends that individuals managing the audit program must consult the audit team Leader in respect of audit team composition, where appropriate,
- Assigning responsibility for a single audit to the audit team Leader,
- Managing audit program results,
- Managing and maintaining audit program record (records related to the audit program, single audits and audit team).

The effective implementation of the audit program involves more than checking that there are no audit delays or audit omissions. It is a more systematic and holistic assessment of whether it is also fit for purpose and controlled.

MONITORING AUDIT PROGRAM

The individuals responsible for managing audit program need to monitor it in order to evaluate if the anticipated results have been achieved.

REVIEWING AND IMPROVING AUDIT PROGRAM

Some audit programs don't vary year to year and an auditor must be concerned when this situation occurs. Audits should, as a rule, be scheduled based on the «status and importance of the activities» as well as «the results of previous audits» and «previous performance». The status and importance of activities will change year by year. Some processes with a history of problems may receive frequent audits, at least until those problems have been resolved, and then the audit intervals may be extended. The strategic priorities of the Organization may change year on year, elevating or decreasing the relative importance of different processes. Therefore, the individuals managing the audit program must actively monitoring of the schedule with the ultimate aim of ensuring that they are using their finite audit resources to maximum benefit. The standard advises that the results of the audit program review must be reported to relevant interested parties.

ର୍ଷ REVISION HINTS ରହ

With reference to ISO 19011, can you:

- Solution with the general components of an audit program?
- Selate the audit program to the PDCA cycle?

STUDENT NOTES

ISO 19011:2018 CONDUCTING AN AUDIT

GENERAL AUDIT PROCESS

ISO 19011 defines the following general audit activities, broken down into stages from initiating the audit to conducting the follow up. Whilst the general process is applicable to all types of audit, the extent and complexity will depend on the auditee, their processes and/or the specific circumstances of the audit. That is, the process will usually be simpler and less formal for a first party audit than for a second or a third party.



STUDENT NOTES

INITIATING AUDIT

The audit team Leader retains the responsibility for conducting the entire lifecycle of the audit until the audit has been completed. Initiating the audit is effectively establishing the ground rules and requirements for the audit. It includes establishing communication channels, methods, resource requirements, roles and responsibilities and so on. It is important at this stage that these parameters and processes are communicated to and understood by all parties involved in the audit (audit client, team members, auditee), in order that the audit objectives can be achieved with maximum efficiency and the minimum of disruption to the auditee's operations. Sometimes this stage may include organizing a preliminary visit to the auditee. This is more common when the auditee organization is large and/or complex, and the audit team leader needs to visit the main sites principally to accurately assess time and specialist resource requirements for the audit. Often these requirements can be established through good pre-audit communication with the auditee, without the need for a visit.

One of the main considerations at this stage is estimating the appropriate time to allocate to the audit. Audit duration will depend on the specific Management System Standard's requirements, the scope of the audit, the size and complexity of operations and the number of auditors in the team. For the audit duration, the accredited Certification Bodies are obliged to follow the requirements of International Standard **ISO 17021-1 (Conformity assessment – Requirements for Bodies providing auditing and certification management systems - Part 1: Requirements)**, specific criteria which have been established for specific certification standards, as well as **IAF (International Accreditation Forum) Mandatory Documents**. The aim is to allocate time consistently to third party audits and ensure that all auditees are audited in a similar way.

In the specific case of the Information Security Management Systems, **ISO 27006** - **Standard specifying requirements, Requirements for bodies providing audit and certification of information security management systems** defines the minimum amount of time that needs to be utilized during a third-party audit. The standard contains a table, depicting a correlation between the number of persons doing work under the organization's control and the ISMS audit time for initial audit. From then on, different parameters could be used in order to reduce or increase the audit time based on complexity.

The parameters that could affect complexity are the following:

Parameters affecting effort	Indicative examples (not exhaustive list)			
Complexity of the ISMS	Only little sensitive or confidential information, low			
 Information security requirements (level of 	availability requirements [reduced effort required].			
security)	Higher availability requirements or some sensitive or			
 Number of critical assets 	confidential information [normal effort required].			
 Number of processes and services 	Higher amount of sensitive or confidential information			
	(e.g. health, PII, insurance, banking etc), or high			
	availability requirements [increased effort required].			
The type of business performed within the scope of the	Low risk business activities without regulatory			
ISMS	requirements [reduced effort required].			
	High regulatory requirements [normal effort required].			

STUDENT NOTES

Parameters affecting effort	Indicative examples (not exhaustive list)
	High risk business with limited regulatory requirements [increased effort required].
Previously demonstrated performance of the ISMS	Recently certified [reduced effort required]. Recent surveillance audit [normal effort required]. No certification and no recent audits [increased effort required].
Extent and diversity of technology utilized in the implementation the various components of the ISMS	 Highly standardized environment with low diversity (few IT platforms, servers, operating systems etc) [reduced effort required]. Standardized but diverse IT platforms, servers, operating systems, databases, systems etc [normal effort required]. High diversity or complexity of IT (many different segments of networks, types of servers or databases, number of key applications etc) [increased effort required].
Extent of outsourcing and third-party arrangements used within the scope of the ISMS	No outsourcing and little dependency on suppliers [reduced effort required]. Several partly managed outsourcing arrangements [normal effort required]. High dependency on outsourcing or suppliers with large impact on important business activities [increased effort required].
Extent of information system development	No in-house system development [reduced effort required]. Use of standardized software platforms with complex configuration / parameterization [normal effort required]. Extensive internal software development activities with several ongoing projects for important business purpose [increased effort required].
Number of sites and number of Disaster Recovery (DR) sites	Low availability requirements and no or one DR site [reduced effort required]. Medium or high availability requirements and no or one DR site [normal effort required]. High availability requirements e.g. 24/7 services [increased effort required].
For the surveillance or re-certification audit: The amount and extent of change relevant to the ISMS	No changes since the last re-certification audit [reduced effort required]. Minot changes in scope of SoA of the ISMS (e.g. some policies and documents) [normal effort required].

STUDENT NOTES

Parameters affecting effort	Indicative examples (not exhaustive list)	
	Major changes in scope of SoA of the ISMS (e.g. new	
	processes, new business units, areas, risk assessment	
	management etc) [increased effort required].	

The duration of an audit day is normally eight (8) hours and may or may not include a lunch break, depending upon local legislation. Auditors' travel time (en-route or between sites), any breaks and time spent by any team member that is not assigned as an auditor (i.e. technical experts, translators, interpreters and auditors in training) are not included in the onsite duration of Management System Certification Audits.

PREPARING AUDIT ACTIVITIES

Performing review of documented information (Stage 1)

Management System standards contain requirements for Organizations to maintain and retain documented information as part of the system. Part of the purpose of conducting the review of documented information is to allow audit team to become familiar with the auditee's Management System so that subsequent audit activities can be better planned. Furthermore, this review allows the audit team to determine the documents' possible conformity with the audit criteria as well as any possible deviations, omissions or conflict of interests. The review must take into account the auditee's context and its size, nature and complexity as well as auditee's related risks and opportunities, the audit scope, criteria and objectives. Furthermore, during this stage the previous internal audits' and Management Review's records are evaluated in order to be estimated the level of implementation of Management System.

The review of documented information is optional for internal audits, particular useful for second party audits and prerequisite for third party audits (Stage 1 is one of ISO 17021-1 & ISO 27006 requirements). The document review does not involve a detailed examination of methods, records, processes etc. but a cursory examination of Management System's effectiveness (context, risk assessment and risk treatment, information security policy and objectives, documented information etc.). The document review adds value to the process for the following reasons:

- It establishes whether it is even worthwhile proceeding to the next stage and onsite audit (stage 2). If an examination of the sufficiency of documentation identifies several omissions or problems, then the audit client must be informed about the issues and resolve them. Afterwards, the onsite audit (stage 2) can be scheduled and conducted.
- It assists the onsite planning processes by familiarising the team with the Management System and, to an extent, the people they will encounter on site. It can assist the audit team by helping them identify key issues for the audit, identify the most appropriate auditee for each process, identify sampling requirements and to allocate an appropriate length of time for each activity.

Especially for the third-party audits, at the end of Stage 1, team Leader will need to make the decision as to whether the onsite audit can proceed. Furthermore, team Leader has to communicate any finding to the auditee immediately after the review has taken place in order that issues may be addressed in advance of the onsite audit. ISO 27006 mandates that a written report is provided to the customer with the conclusion of Stage 1.

STUDENT NOTES

Moreover, the certification body shall review the stage 1 audit report before deciding on proceeding with stage 2 and shall confirm if the stage 2 audit team members have the necessary competence.

Audit planning

Depending on the size and complexity of the auditee Organization, this can be a real test of the Lead auditor's organizational capabilities. For example, if the Organization is large, has complex operations and several sites miles apart, all doing different things, and the audit will last a week and involve a team of four (4) auditors, the Lead Auditor has to find a way of achieving the audit objectives with maximum efficiency. When planning the audit, the team Leader must consider the composition and overall competence of the audit team, which sampling techniques are appropriate, any opportunities to improve the effectiveness and efficiency of the audit activities and any risks to the auditee arising as a result of the audit being conducted.

However, there will also be a large number of logistical issues to consider, such as the following:

- Minimizing time lost due to travel between sites
- Accommodations and travel expenses
- The most efficient sequence of audit activities
- Audit team communication throughout the audit
- Periodical communication of the audit progress and any concerns to the audit client, by the team Leader

At this stage it is important that the audit team Leader must remember that the Audit Plan is a working document not just for the audit team, but also for the auditee, so it must be agreed with them well in advance, so people can be ready, and also in a readily understandable format. The audit plan will still need to be sufficiently detailed and understandable to enable effective co-ordination of auditors and auditees throughout the duration of the audit. In simple terms, the main purpose of the audit is to ensure that the right people are in the right locations at the right time to be audited on a subject they have been informed of in advance.

On the following page, an example of an audit plan can be found.

The example shows an audit plan for a small single site logistics organisation, over a period of 2 days, carried out by a sole auditor. The organization excludes all controls from A.14. from its ISMS implementation. It is therefore a very simple example. An audit plan for a large, multi-site, complex organisation, involving a team of 2 or more auditors will be much more complex.

STUDENT NOTES

Audit plan (simple example, 1 auditor, 2 calendar days)

AUDITED ORGANISATION	ACME Ltd.
DATE OF AUDIT	2-3 September
AUDIT CRITERIA	ISO 27001:2022
AUDIT SCOPE	ISMS that covers the company services
AUDITOR	Mr. Great Auditor
AUDIT OBJECTIVE	<i>To determine and report the extent of conformance of the management system of ACME Ltd. to ISO 27001 requirements</i>

AUDIT TIMETABLE			
DAY 1		DAY 2	
08:45-09:00	Induction		Segregation of duties within key roles of
09:00-09:30	Opening meeting with ACME Ltd. management team	08:45-09:30	Contact with authorities and groups Mobile devices and teleworking (Interview with IT and Information Security Managers and any other appropriate personnel).
09:30-10:30	Top management activities and Risk Management, information on compliance (interview with the General Manager and the Information Security Manager)	09:30-10:30	Asset Management (including information classification) Cryptographic controls (Interview with IT and Information Security Managers and any other appropriate personnel).
10:30-10:45	Break	10:30-10:45	Break
10:45-12:30	Roles, competencies, responsibilities and authorities HR functions with relevance to information Security (e.g. selection, onboarding, training, off-boarding) (interview with the HR manager and any other appropriate personnel)	10:45-12:30	Access Control Management Network Security Management (Interview with IT and Information Security Managers and any other appropriate personnel).
12:30-13:15	Lunch	12:30-13:15	Lunch
13:15-14:00	Change Management as part of the system's operation. (Interview with IT and Information Security Managers).	13:15-14:00	<i>Operations Security (Interview with IT and Information Security Managers and any other appropriate personnel).</i>

STUDENT NOTES

AUDIT TIMETABLE			
14:15-15:00	Outsources processes and supplier management (Interview with Procurement, IT and Information Security Managers).	14:15-15:00	Information security in project management (Interview with project management team)
15:00-15:15	Break	15:00-15:15	Break
15:15-16:30	Personnel awareness Physical and environmental security (site tour and interviews with a sample of organization's staff)	15:15-16:30	Information security incident management Information security aspects of business continuity management (Interview with IT and Information Security Managers and any other appropriate personnel).
16:45-17:00	End of day update (Discussion with the Information Security Manager)	16:45-17:00	Closing meeting with Top Management

Preparing documented information for audit

The auditors must collect and review information, according to their audit assignments, and prepare documented information for the audit, using any appropriate media. These can include physical or digital checklists, audit sampling details etc.

The conduct of audit is based on records' sampling process, so by definition the audit will always miss something. However, it is unforgivable to fail to evaluate an important area of risk or a key requirement. A well thought out checklist reduces the chances that something important will be missed, forgotten about or overlooked. The checklist is an "aide memoir" (French meaning an aid for the memory) and a working document for the auditors and must be understandable to the user. The auditor must avoid slavishly following the checklist and failing to follow audit trails that open up as the audit progresses.

Checklist (example)

AUDIT CHECKLIST		
DATE	3 September	
AUDIT OF	ACME Ltd.	
AREA UNDER REVIEW	Change Management as part of the system's operation.	
AUDITEE	Ms. Great Auditee	
AUDITOR	Mr. Great Auditor	

STUDENT NOTES

ASSESSMENT QUESTIONS	CONFORMS?	COMMENTS
Is there a specific procedure for the management of		
changes within the information security management		
system? Is the procedure accompanied by specific		
forms or other records that need to be retained? (8.1.,		
A.12.1.2.)		
Has the procedure been followed for a sample of		
specific changes? (8.1., A.12.1.2.)		
Have the relevant files been correctly completed and		
maintained? (7.5.)		
Have there been any unintended changes? Has the		
organization reviewed the consequences of these		
changes? Has the organization taken action to		
mitigate any adverse effects as necessary? (8.1.,		
A.12.1.2.)		
Have any information security incidents occurred		
because of the implementation of changes? (A.16)		
Have major changes affecting information security		
been discussed during management review? (9.3.)		

Auditor's signature:

CONDUCTING AUDIT ACTIVITIES

Effective planning reduces the chances of problems onsite, however, if the auditors lack discipline and focus then the audit objectives may not be achieved. A successful on-site audit will involve an effectively managed and executed process, as well as demonstration of the necessary auditors' skills and competencies.

Conducting Opening Meeting

The purpose of the opening meeting, usually conducted by the audit team Leader and delivered in the presence of senior management of the auditee Organization, is to provide a short explanation of how the audit activities will be undertaken, to create transparency in the process, ensure everyone knows what to expect and what co-operation the team will need, and finally to give the auditee an opportunity to ask questions. There is a sample agenda for an Opening Meeting below (adapted from ISO 19011: 2018 and ISO/IEC 17021-1).

STUDENT NOTES

TYPICAL OPENING MEETING AGENDA (ADAPTED FROM ISO 19011 AND ISO/IEC 17021-1)

- Introduction of the participants, including an outline of their role
- Confirmation of audit plan, (including type and scope of audit, objectives and criteria), any changes, and other relevant arrangements with the client, such as date and time of closing meeting, interim meetings between the audit team and the auditee's management
- Sconfirmation of formal communication channels between the audit team and the auditee
- Solution that the resources and facilities needed by the audit team are available
- Solution of matters relating to confidentiality and information security
- Sconfirmation of relevant work safety, emergency and security procedures for the audit team
- Confirmation on relevant access, health and safety, security, emergency and other arrangements for the audit team
- by The method of reporting, including any grading of audit findings
- Methods and procedures to be used to conduct the audit based on sampling
- Sconfirmation that, during the audit, the auditee will be kept informed of audit progress and any concerns
- 🤟 Information about the conditions under which the audit may be prematurely terminated
- Any system for feedback from the auditee on the findings or conclusions of the audit, including complaints or appeals

Guides

Guides are assigned to the audit team to facilitate the audit, especially if the site being audited is large, complex, dangerous, has parts here access is restricted, or where special clothing or Personal Protective Equipment (PPE) is required. The responsibilities of a guide can include: establishing contacts and timing for interviews, arranging visits to specific parts of the site or Organization, 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 auditee, providing clarification or information as requested by an auditor etc. In some cases, the auditee can act as guide and especially a Division Manager from auditee Organization.

COLLECTING AND VERIFYING INFORMATION

Both ISO 19011 and ISO/IEC 17021-1 identify two important aspects at this stage of the onsite process. Collection and verification. The auditor may generate lots and lots of information from a wide range of sources using techniques such as interviews, review of documentation and records and observation of processes and activities, but it is critical that this all leads to decisive conclusions regarding the degree of conformance to the audit criteria.

STUDENT NOTES

Only information that can be subject to some degree of verification can be accepted as audit evidence. Where the degree of reliance is low the auditors must use their professional judgment to determine the degree of reliance that can be placed on it as evidence. Therefore, the auditor must continually review the evidence as it comes, compare it continually with the criteria, clarify it as necessary with the auditee, and stop when enough evidence (one way or the other) has been found. Apparent non-conformities should be discussed with the auditee at the point of discovery.

There are three good reasons for this:

- It gives the auditee a chance to explain the situation if the auditor has misinterpreted the evidence.
- It reduces the chances of argument in the Closing Meeting if a series of findings that were not discussed are delivered.
- It is «professional behavior» and helps maintain good relations during the audit if there is transparency.

As the audit progresses, the auditors must decide on the conformance degree of Management System with the audit criteria.

Below, there is a figure from ISO 19011 which provides an overview of a typical process from collecting information to reaching audit conclusions.



STUDENT NOTES

GENERATING AUDIT FINDINGS

Once information has been collected and verified, the audit team will need to summarise the collection of verified information into a set of audit findings. This may involve grading the non-conformities (e.g. major or minor) and deciding what the overall conclusion should be in light of any non-conformities found.

If the audit is being carried out by a team, this stage will require an organised communication and consensus process within the team. Findings should contain sufficient information to enable the recipient to understand and to appreciate that the auditor has reached the right conclusion (i.e. reference to the criteria and the evidence).

An example of a well written report is given below. Notice how the body of the report contains three key pieces of information:

- What the criteria requires
- What actually happened
- The supporting evidence

Also notice how it is written in simple, clear language for the benefit of the auditee.

Non-conformity report (example)

CPA CERTIFICATION: NON-CONFORMITY REPORT		
NCR No.	1	
ISO 27001 CLAUSE	8.1. – Operational Planning and Control	
NON CONFORMITY	Major / Minor / Observation	
CATION OF NON-CONFORMITY OR Change Management as part of the system's operation.		
OBSERVATION (I.E. DEPT/SITE)	SERVATION (I.E. DEPT/SITE) IT Department	
DESCRIPTION OF NON-CONFORMITY		

ISO 27001 Clause 8.1. requires that the organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

It is established that ACME Ltd. has documented a Change Management procedure detailing the steps, roles and records that need to be followed when a change needs to be implemented.

During the audit it was established that for the change related to the replacement of the access control system of the organization, the above-mentioned procedure was not followed and no relevant records were created. In this case, the Information Security Manager of the organization was not notified and no information security implications were identified (as prescribed by the procedure).

Evidences

documented a Change Management procedure no relevant records were created

STUDENT NOTES

CORRECTIVE ACTION DETAILS AND TIMESCALE FOR COMPLETION

ISSUED BY (Auditor)

ACCEPTED BY (Company Representative)

Notice how the area reserved for "corrective action" is empty. This is because, when the report is issued by the auditor, the corrective action, as an auditee responsibility, has yet to be determined. This <u>may</u> be filled in during the Closing Meeting.

CLASSIFICATION OF NON-CONFORMITIES

It is common for the client to request that non-conformities are graded to reflect their severity and relative urgency for corrective action to be taken. Different clients have different classification systems. Most systems, however, are variations on the theme detailed in the example below.

GRADING	DING WHAT DOES THIS MEAN?	
Major	A big problem. There may be a significant part of the audit criteria that has not been met (e.g. a major non-conformance to clause 9.2 could be that no internal audits have been completed for a year or more). Non-conformities that have had a tangible impact on information security are also generally graded as major due to the potential for immediate adverse impact on the organization or its customers. Major non-conformities require corrective action to be taken as a matter of urgency, as they are likely to be harming the company with each day that they remain open	
Minor	A smaller problem. There may be a part of the audit criteria that has not been FULLY met (e.g. a minor to clause 9.2 could be a 2-month backlog of internal audits, or a small number of corrective actions that have gone beyond their agreed deadlines for corrective action). Minor non-conformities generally affect internal operations and efficiency, with little or no immediate impact on information security or customer. Corrective action is required (as the problem can escalate) however minor non- conformities are not generally treated as matters of urgency, and may be given a more generous timescale for completion.	
Observation/Opportunity for Improvement	A "nearly" problem or inefficiency. An observation or OFI (Opportunity of improvement) is NOT a non-conformity and therefore does NOT require mandatory corrective action. It can be described as an instance where a system is "working but wobbling". Requirements are being met – but only just. Observations are raised when an auditor sees a value in bringing the matter to the auditee's attention, but	

STUDENT NOTES

corrective action is taken at the auditee's discretion. The auditor will generally keep observations in view, as they have the potential to become non-conformities if the situation deteriorates. Auditors may also raise observations on apparent problems observed during the audit that were outside the scope of the audit being performed (e.g. possible health & safety breaches)

It is important that non-conformities should only be raised when they can be supported by <u>clear objective evidence</u> and the evidence shows <u>a clear breach against the audit criteria</u> (small or large). If an auditor has any doubt, then a non-conformity must not be raised. All doubts should have been cleared before pen is put to paper, otherwise there is a risk that the non-conformity is not factually correct and invalid.

PREPARING AUDIT CONCLUSION

The audit objectives and audit findings must contain a clear and reliable conclusion, otherwise it will be unclear whether the audit objectives have been achieved. ISO 19011 provides the following guidance on developing audit conclusion:

Content of audit conclusions

Audit conclusions can address issues such as the following:

- 1. The extent of conformity with the audit criteria and robustness of Management System, including the effectiveness of Management System in meeting the intended outcomes, the identification of risks and effectiveness of actions taken by auditee to address risks,
- 2. The effective implementation, maintenance and improvement of Management System,
- 3. Achievement of audit objectives, coverage of audit scope and fulfillment of audit criteria,
- 4. Similar findings made in different areas that were audited or from a joint or previous audit for the purpose of identifying trends.

If specified by the audit plan, audit conclusions can lead to recommendations for improvement or future auditing activities.

CONDUCTING CLOSING MEETING

The formality of the Closing Meeting will depend on the nature of the audit. In general terms, the Closing Meeting is a presentation of the findings by the auditor to the auditee and its objectives are to establish agreement between the two parties that the findings are understood, accepted and to secure a commitment to appropriate corrective action, if nonconformities have been reported. Frequently, during the meeting, the nature of corrective action will be discussed, agreed and documented.

However, sometimes the auditee needs to have a period of time to evaluate the problem cause and submit a proposal for corrective action within an agreed timeframe.

STUDENT NOTES

For some audits, the Closing Meeting is formal (mostly for second- and third-party audits) and minutes, including records of attendance, can be kept.

The audit team Leader can increase the effectiveness of the Closing Meeting by taking the following precautions:

- Clearly reference the audit findings to the audit criteria (explain it in simple terms if necessary)
- Clearly identify and explain the specific objective evidence that supports the audit findings
- Do not raise any findings (especially nonconformities) that were not discussed fully and agreed with the auditee at the point of discovery.

Any diverging opinion regarding the audit findings or conclusions between the audit team and the auditee must be discussed and, if possible, resolved. If not resolved, this should be recorded.

Typical closing meeting agenda items

It is important that the audit team Leader prepares a closing metering agenda in order to ensure that all important aspects will be mentioned and none of them will be left uncovered or unexplained.

Typically, the agenda will include:

- Introductions and thanks
- Affirmation of audit scope, objectives and criteria
- Description of the process that was followed and any difficulties encountered
- The audit evidence obtained was based on sample of the information available
- Presentation of audit findings and conclusions
- Establish agreement on findings and commitment for the implementation of corrective actions, if needed
- Explain about of post-audit activities.

PREPARING AND DISTRIBUTING AUDIT REPORT

The audit team Leader who is responsible for audit report content must ensure that the audit report is prepared before the Closing Meeting (typical for third party audits). Usually, the audit report is presented at the Closing Meeting and is some cases, it may be prepared after the Closing Meeting and distributed to the auditee and audit client within an agreed period of time after the audit has finished. If this is the case, then a verbal summary of the likely contents of the formal report must be presented at the Closing Meeting. The audit report must clearly identify type of audit, scope, objectives, criteria, findings, conclusions, significant issues impacting on the audit program, dates and places where the audit activities were conducted, any deviation from the audit plan and their reason, participants, distribution, any disagreements or significant problems (in process) that were encountered etc. The audit team Leader must remember that the purpose of the audit report is to accurately identify the degree of conformity with audit criteria. A failure to report areas of conformance is a major omission.

ISO 19011 advises that audit report must be distributed to relevant interested parties as defined in the audit program or audit plan.

STUDENT NOTES

Summary report (simple example)

AUDIT SUMMARY REPORT		
COMPANY NAME	ACME Ltd.	
DATE OF AUDIT	2-3 September	
AUDITOR (S)	Mr. Great Auditor	
AUDIT SCOPE	ISMS that covers the company services	
AUDIT CRITERIA	ISO 27001:2022	
TYPE OF AUDIT	Initial Certification	

SUMMARY OF FINDINGS

Over the course of the 2 day audit all key operational and management processes were sampled.

The 3 minor non-conformances that were raised during the initial assessment had been effectively cleared by the time of the onsite audit and these have now been closed. Operational processes were sound with good record keeping, communications, induction and training systems in place. Risk management activities are implemented and communicated within the organization. Risk treatment plans have been designed and are on going. The organization has documented a procedure for the management of change, but for the change related to the replacement of the access control system, it has not been followed (see NCR1 attached).

The organization has set information security objectives and has instigated specific KPIs at different levels to facilitate the monitoring of the system. Although the system is at its early stages of implementation (counting only 6 months of full operation), the organization has extracted information regarding the monitoring and measurement of the various processes and reached conclusions regarding the effectiveness of the system. Corrective actions are implemented and no information security incidents have been documented. The various controls are implemented as described in the various policies and procedures and in alignment with the Risk Management information.

Overall a good level of conformance to ISO 27001 was demonstrated, with good levels of staff awareness and commitment shown from the top.

RECOMMENDATION

It is recommended that certification to ISO 27001 be awarded subject to the submission of an acceptable corrective action plan relating to the three minor non-conformance.

ISSUED BY (Auditor)	Great Auditor
ACCEPTED BY (Company Representative)	Great Auditee

STUDENT NOTES

COMPLETING AUDIT

The audit is complete when all planned audit activities have been carried out and the documented information pertaining to the audit has been retained and distributed, according to the agreement between the participating parties. Concerning the maintenance of records on the audit, accredited Certification Bodies (third party audits) are obliged to follow the requirements of ISO/IEC 17021-1 but the audit plan and the audit report will always be retained, in contrast to audit checklists. Any information obtained during the audit, or audit report, must always be kept confidential unless there is a legal requirement to disclose. In this case, the audit client and the auditee must be informed as soon as possible.

Lessons learned from the audit can identify risks and opportunities for the audit program and the auditee.

CONDUCTING AUDIT FOLLOW-UP

In the event that corrective actions or corrections form part of the audit findings, the auditee will liaise with the individuals managing the audit program and/or audit team with regard to the status and progress of these agreed actions. These actions are not considered part of the audit, however, the completion and effectiveness of these actions must be verified by the original audit team.

It is the responsibility of the auditee to identify and implement the necessary corrective actions (not the auditor) for the following reasons:

- The auditor needs to remain independent to the working processes
- The auditor is unlikely to have access to all the appropriate technical knowledge surrounding the problem area, and not best placed to decide how any problem should be fixed
- There is a better chance of an effective and "owned" (as opposed to an imposed) solution

Details of the auditor's judgement on the sufficiency or otherwise of actions taken must be reported to the individual managing the audit program and reported to the audit client for Management Review.

STUDENT NOTES

ର REVISION HINTS ର

With reference to ISO 19011, can you:

- Solution the general audit process from initiating the audit through to follow up activities?
- Explain the purpose of each stage and typical stage activities (e.g. the Stage 1 Audit, Stage 2 Audit)?
- Udentify the key responsibilities of the lead auditor before, during and after the audit?
- Explain who is responsible for what at each stage (e.g. corrective action, follow up)?
- Explain how the process may differ between first, second- and third-party audit?
- Udentify the stages of the audit when Top management from the auditee Organization should be present?

STUDENT NOTES

ISO 19011 COMPETENCE OF AUDITORS

GENERAL

Confidence in the audit program depends to a significant degree on the competence of those individuals involved in the audit process. ISO 19011 separates the requirement «auditor competence» into two important aspects. These are the following:

- Personal behaviour
- Possession of necessary knowledge and skills and the ability to apply them consistently

This section clarifies the specific requirements of ISO 19011, relating to the two aspects of auditor competence.

PERSONAL BEHAVIOUR

What are the personal attributes that make a good auditor? Can anyone be a good auditor? The fact that most people will have encountered both good ones and bad ones suggest that it is not an occupation that comes easily to everyone. ISO 19011 identifies a number of **desired** attributes that a good auditor must possess and demonstrate. These are:

ETHICAL CONDUCT	OPEN-MINDEDNESS	DIPLOMACY
Fair, truthful, sincere, honest, discreet	Open to consider alternative ideas or different points of view	Tactful in dealing with individuals
OBSERVATION	PERCEPTIVENESS	VERSATILITY
Actively observing physical	Able to interpret situations	Able to adjust to different
surroundings and activities	accurately	situations
ΤΕΝΑCITY	DECISIVENESS	SELF-RELIANCE
Persistent and focussed on	Able to reach timely conclusions	Able to act and function
achieving the audit objectives	based on logical reasoning and	independently while interacting
, ,	analysis	effectively with others

KNOWLEDGE AND SKILLS

Audits require a certain amount of knowledge and skills which are separated into main aspects:

- The knowledge and skills necessary to achieve their intended results
- Generic competence and level of discipline and sector-specific knowledge and skills

STUDENT NOTES

Generic knowledge and skills of auditors

THE ABILITY TO APPLY AUDIT PRINCIPLES,	AN UNDERSTANDING OF MANAGEMENT SYSTEM		
PROCESSES AND METHODS	STANDARDS AND OTHER REFERENCES		
In short, the audits are performed in consistent and systematic manner by the auditor who, among others, must have the ability to understand the types of risks and opportunities associated with auditing and the principles of the risk-based approach to auditing	The auditor must have the ability to understand how the auditee has applied the Management System standard(s) to their Organization, the relationships and interactions between processes and the importance and respective priority of multiple standards or references. Furthermore, the auditor must have the ability to understand the application of standards or reference documents to different audit situations.		
AN UNDERSTANDING OF THE AUDITEE	A KNOWLEDGE OF APPLICABLE STATUTORY AND		
ORGANIZATION AND ITS CONTENT	REGULATORY REQUIREMENTS AND OTHER		
CINEARIZATION AND ITS CONTENT	REQUIREMENTS		
The auditor must have the ability to understand the auditee's structure, purpose and management practices, including an understanding of the needs and expectations of relevant interested parties that impact	The auditor must have the ability to work within the auditee's applicable legal and statutory framework, including other requirements which may be imposed. Furthermore, he or she must have the ability to understand the statutory and regulatory requirements and their governing agancies, basis legal terminology		

the management system

and their governing agencies, basic legal terminology and contracting and liability law, in relation to the auditee's activities, processes, products and services.

Discipline and sector - specific competence of auditors

ISO 19011 advises that audit teams must have the collective discipline and sector-specific competence appropriate for auditing the particular types of Management Systems and sectors.

The discipline and sector-specific competence of auditors must include knowledge of: Management System requirements and principles and their application; fundamentals of the discipline(s) and sector(s) related to the management system standards as applied by the auditee; application of discipline and sector specific methods, techniques, processes and practices which permit the team to assess conformity within the defined audit scope and to generate appropriate audit findings and conclusions as well as principles, methods and techniques which are relevant to the discipline and sector, such that the auditor is able to determine and evaluate risks and opportunities associated with the audit objectives.

STUDENT NOTES

Third party Certification Bodies use a set of industry codes (European Accreditation Codes), according to Regulation (EC) No 1893/2006 of the European Parliament and the Council of 20 December 2006 and IAF Informative Document ID1, to help them match the right auditor to the right audit. In ISMS audits, the specific competencies are further defined based on ISO 27006. (more information is provided below).

GENERIC COMPETENCE OF AUDIT TEAM LEADER

The audit team Leader is not necessarily the oldest, most experienced or most technically aware auditor in the team. The audit team Leader is that person who has leadership skills to manage the audit team and achieve the audit objectives as well as to facilitate the efficient and effective conducting of audit. Furthermore, he or she is prepared to take on the extra work that goes with the job.

ŀ	ADDITIONAL COMPETENCE REQUIREMENTS		EXTRA WORK
•	Plan the audit and assign audit tasks according to the specific competence of individual audit team members	•	Liaising with the audit client before (in connection with the plan, team selection etc) and after the audit (submitting reports, explaining the findings)
Ì	Discuss strategic issues with top management of the auditee to determine whether they have considered these issues when evaluating their risks and opportunities	•	Liaising with the auditee before the audit (in connection with the plan, answering questions)
•	Develop and maintain a collaborative working relationship among audit team members	•	Resolving disputes, disagreements, chairing meetings etc
•	Manage the audit process including making effective use of resources, managing the uncertainty of achieving audit objectives, protecting the health and safety of the audit team members etc.	•	Sorting out travel and accommodation issues of audit team with the audit client
•	Represent the audit team in communications with individuals managing the audit programme, the audit client and the auditee	•	More paperwork before and after the audit
•	Lead the audit team to reach decisive conclusions		
•	Prevent/resolve conflict and problems		
•	Understand the requirements of each of Management System standards being audited and recognize the limits of their competence in each of the disciplines		
•	Preparation of the final report and its distribution		

STUDENT NOTES

Ultimately the audit team Leader is at the center of a triangle that includes the client, the auditee and the audit team. The audit team Leader has to appreciate the needs of each party and strike a balance between their needs whilst maintaining a clear focus on achieving the audit objectives.

SPECIFIC COMPETENCE OF AUDIT TEAM MEMBERS

Based on ISO 27006, the audit team members should have at least:

- Knowledge of information security
- ⇒ Technical knowledge of the activity to be audited

- Schweizer Schwei

More specifically, the audit team members should have at least:

- a) Professional education or training to an equivalent level of university education.
- b) Has at least four years full time practical workplace experience in formation technology, of which at least two years are in a role of 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 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.
- 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.

CONDUCTING AUDITOR EVALUATION

When an auditor works for a third-party Certification Body he or she will be evaluated as competent to audit Organizations in certain industries (depending on the auditors' background and experience). Both ISO 19011 and ISO/IEC 17021-1 suggest several evaluation methods for auditors as: review of records which verify the auditor background, feedback from past employers about auditor performance, individual interviews, observation of his or her audit activities, written examinations etc.

STUDENT NOTES

ର REVISION HINTS ର

With reference to ISO 19011, can you:

- Identify at least 6 desirable personal attributes for an auditor.
- Udentify the important competence and knowledge requirements for an ISMS auditor.
- Udentify the additional competences that a Lead auditor must demonstrate.
- Udentify the additional workload requirements of the lead auditor.
- Explain what sort of specific knowledge that an auditor may need to possess when auditing in different sectors? (e.g. telecommunications vs a logistics company vs a company with an extended OT environment)

STUDENT NOTES

ACCREDITATION, CERTIFICATION AND ISO 17021

CERTIFICATION BODIES AND THE GREEK ACCREDITATION SERVICE (ESYD)

A 3rd party assessment to an international standard such as ISO 27001 may be through an accredited or nonaccredited certification scheme. Often it may be a requirement of a customer that the supplier is certificated (or registered), and it is often also a requirement that certification is accredited. But what does that mean?

Well, both there are companies that call themselves "certification bodies" that offer certification to international standards, and it is those companies that are either accredited or not. These certification bodies employ auditors to independently assess companies to a standard and (providing the results are favourable) issue a certificate at the end of the process. With a non-accredited certification body, the process stops there. That is, there is no independent check on the integrity of the process or certificate, and the non-accredited certification body is accountable only to themselves. With "accredited certification" there is. The certification body is subsequently accountable to the accreditation body for the integrity of the process and the award (in Greece, the accreditation body is ESYD). Because of the extra level of independent scrutiny, accredited certification generally carries more currency than non-accredited. In fact, many customers do not recognise non-accredited certificates.

Among other things, ESYD assesses the independence, integrity and technical competence of certification bodies in Greece that apply for accreditation against the requirements of **ISO 17021 (Conformity assessment -Requirements for bodies providing audit and certification of management systems)** – Therefore when ESYD performs an audit on a third-party certification body, the audit criteria they use is ISO 17021.

Companies and organisations that are accredited by ESYD, can be identified easily as their certification logos bear the ESYD logo. Similarly, companies and organisations accredited by the UK UKAS accreditation service, UKAS, are identified by the UKAS logo. The certified firm can display these logos on its publicity material. The number at the bottom of the logo is unique to each accredited certification body.

Examples of companies accredited by ESYD and UKAS to provide accredited certification to ISO 27001 in Greece or the UK are:

- BSI
- EUROCERT
- LRQA
- QMSCERT
- SGS
- TÜV Austria Hellas
- TÜV Nord Germany Hellas





000