Raad voor Accreditatie
(Dutch Accreditation Council RvA)

Explanation concerning the implementation of ISO/IEC 27006:2015

Document code:	**RvA-T045-UK**
	Version 1, 10-10-2016

An RvA Explanation describes the policy and/or the RvA procedure with regard to a specific accreditation topic. If the policy and/or the procedure concerning an accreditation topic that is described in an RvA Explanation are/is recorded in an EA, ILAC or IAF document, the RvA shall harmonise its policy or procedure with that EA, ILAC or IAF document.

An up-to-date version of the Explanation can be obtained via the RvA website (www.rva.nl).

Contents

1 Introduction

This Explanation is applicable to all management system accreditations (ISO/IEC 17021-1), with ISO 27001 as scope, that are assessed using ISO/IEC 27006.
The ISO/IEC 27006:2015 standard “Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems” has been published on 1 October 2015. This standard replaces the ISO/IEC 27006:2011 standard with the same title.
The International Accreditation Forum (IAF) has decided that there will be a period of 2 years for the transition from ISO/IEC 27006:2011 to ISO/IEC 27006:2015, in other words up to 1 October 2017.
The changes concern first and foremost the references to or amendments to ISO/IEC 17021-1:2015. In addition, the changes concern new text which adds new requirements, and changes to the text of ISO/IEC 27006:2011 that reformulate the requirements.
The changes relating to ISO/IEC 17021-1:2015 are not stated separately, despite the fact that the changes relate to ISO/IEC 27006:2011 (for example the competency requirements).
This Explanation describes the RvA policy and the RvA procedure relating to assessments against ISO/IEC 27006:2015, the making of accreditation decisions against this new standard and the replacement of the accreditation declarations and the scopes of the accreditation.

After 1 October 2017, the accreditation for management system certification for information security in accordance with ISO/IEC 27001:2013 is only possible if the body is in possession of an accreditation in accordance with ISO/IEC 17021-1:2015 and complies with the ISO/IEC 27006:2015 requirements.

2 Transition arrangements

2.1 General

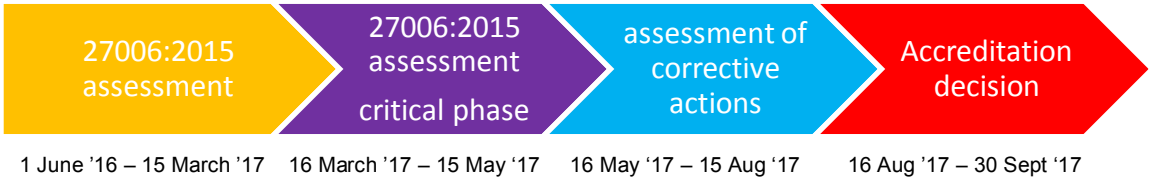
The RvA applies the basic principle that the RvA assessments against the new and amended requirements contained in the new standard shall be conducted as much as possible during the regular assessments. The RvA has detailed the transition arrangements for the implementation of ISO/IEC 27006:2015 below.

New accreditation requests:
ISO/IEC 27006:2015 shall be used from 1 June 2016 for new accreditation requests.

Existing accreditations:
1. Annex A contains a comparison between ISO/IEC 27006:2011 and ISO/IEC 27006:2015. The new and amended requirements in ISO/IEC 27006:2015 are stated explicitly in that comparison.
2. From 1 June 2016 the RvA shall conduct the regular assessments against the requirements contained in ISO/IEC 27006:2015. Section 2.2 contains details about the assessment procedure.

3. Special corrective action provisions are applicable for non-conformities established against new and/or changed requirements during assessments between 1 June 2016 and 15 March 2017, which would not have been reported as non-conformities against the requirements of ISO/IEC 27006:2011. These special provisions are described in Section 2.3 of this Explanation.
4. The RvA shall issue an amended annex to the accreditation declaration after compliance with ISO/IEC 27006:2015 has been established, a positive decision has been made and an accreditation declaration has been issued, or will be issued simultaneously, for ISO/IEC 17021-1:2015.
5. If this decision cannot be made before 1 October 2017 the scheme concerning management system certification for information security in accordance with ISO/IEC 27001:2013 shall be removed from the annex to the accreditation declaration.
6. The managing board of the RvA shall determine the procedure for situations that deviate from the situations set out above.

The timeline for the transition is shown schematically below.



2.2 RvA assessment of the transition to ISO/IEC 27006:2015

The RvA shall assess the implementation of the new and changed requirements in the following way:

- By assessing documents during and in preparation for the transition assessment the assessment team shall verify whether the new and changed requirements are adequately incorporated in the documented management system. For this purpose, the body shall make available to the assessment team a cross-reference list between the requirements stated in Annex A and its own documented management system.
- On the basis of the body's internal audits and management reviews the assessment team shall verify whether the body has itself established the implementation of the new and changed requirements.
- The assessment team shall verify the implementation on the basis of a dossier assessment, interviews and observations of activities.

2.3 Non-conformities against the new requirements

Non-conformities against the requirements of ISO/IEC 27006:2015 that would not have been regarded as such under ISO/IEC 27006:2011 shall be categorised in the assessments between 1 June 2016 and 15 March 2017 as (B) non-conformities. Annex A to this Explanation specifies the requirements against which a (B) non-conformity can be formulated. The body has the opportunity until 16 May 2017 to implement corrective actions and to submit the report on that implementation to the RvA (see RvA-BR004). The RvA shall assess those actions and the assessment team shall issue its advice to the

managing board of the RvA by no later than 15 August 2017. The managing board of the RvA shall make the accreditation decision before 1 October 2017.

If the RvA is unable to make a positive decision regarding the granting of ISO/IEC 27006:2015 accreditation before 1 October 2017 because it has not been possible to close the non-conformities, the management system certification scheme for information security in accordance with ISO/IEC 27001:2013 will be removed from the annex to the accreditation declaration with effect from 1 October 2017.

3 Changes with regard to the previous version

None. This is the first version of this explanatory document.

Annex A: List of changes

Article	Change
all	Reference to ISO/IEC 27006:2015
5.2.1	The requirements regarding conflicts of interest have not significantly changed. The fact that CBs can carry out the duty of certification, including information meetings, planning meetings, examination of documents, auditing (not internal ISMS auditing or internal security reviews) and follow up of non-conformities, without this being considered as consultancy or having a potential conflict of interest is no longer mentioned.
7.1.2.1.1	The general requirements with regard to having criteria for verifying the background experience, specific training or briefing of audit team members, have been changed. These criteria shall ensure at least: a) knowledge of information security; b) technical knowledge of the activity to be audited; c) knowledge of management systems; d) knowledge of the principles of auditing; e) knowledge of ISMS monitoring, measurement, analysis and evaluation. These above requirements a) to e) apply to all auditors being part of the audit team, with the exception of b), which can be shared among auditors being part of the audit team.
7.1.2.1.2	With regard to Information security management terminology, principles, practices and techniques, it is required that: Collectively, all members of the audit team shall have knowledge of: a) ISMS specific documentation structures, hierarchy and interrelationships; b) information security management related tools, methods, techniques and their application; c) information security risk assessment and risk management; d) processes applicable to ISMS; e) the current technology where information security may be relevant or an issue. Every auditor shall fulfil a), c) and d).
7.1.2.1.3	With regard to information security management system standards and normative documents, the requirements have been changed and made more specific. It is required that: Auditors involved in ISMS auditing shall have knowledge of: a) all requirements contained in ISO/IEC 27001. Collectively, all members of the audit team shall have knowledge of: b) all controls contained in ISO/IEC 27002 (if determined as necessary also from sector specific standards) and their implementation, categorised as: 1) information security policies; 2) organisation of information security; 3) human resource security; 4) asset management; 5) access control, including authorisation; 6) cryptography; 7) physical and environmental security; 8) operations security, including IT-services; 9) communications security, including network security management and information transfer; 10) system acquisition, development and maintenance; 11) supplier relationships, including outsourced services; 12) information security incident management; 13) information security aspects of business continuity management, including redundancies; 14) compliance, including information security reviews.

Article	Change
7.1.2.1.4	With regard to Business management practices, it is required that: Auditors involved in ISMS auditing shall have knowledge of: a) industry information security good practices and information security procedures; b) policies and business requirements for information security; c) general business management concepts, practices and the inter-relationship between policy, objectives and results; d) management processes and related terminology.
7.1.2.1.5	With regard to Client business sector, it is required that: Auditors involved in ISMS auditing shall have knowledge of: a) the legal and regulatory requirements in the particular information security field, geography and jurisdiction(s); b) information security risks related to business sector; c) generic terminology, processes and technologies related to the client business sector; d) the relevant business sector practices. The criteria a) may be shared amongst the audit team.
7.1.2.1.6	With regard to Client products, processes and organisation, it is required that Collectively, auditors involved in ISMS auditing shall have knowledge of: a) the impact of organisation type, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing; b) complex operations in a broad perspective; c) legal and regulatory requirements applicable to the product or service.
7.1.2.3.3	With regard to competence requirements for conducting the application review, requirements related to client products, processes and organisation have been determined: Personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of: a) client products, processes, organisation types, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing functions.
7.1.2.4.2	With regard to competence requirements for personnel reviewing audit reports and making certification decisions, it is required that they shall have knowledge of: a) the items listed in 7.1.2.1.2 a), c) and d); b) legal and regulatory requirements relevant to information security.
7.2.1	The requirements regarding demonstration of auditor knowledge and experience have been changed. The certification body shall demonstrate that the auditors have knowledge and experience through: a) recognised ISMS-specific qualifications; b) registration as auditor where applicable; c) participation in ISMS training courses and attainment of relevant personal credentials; d) up to date professional development records; e) ISMS audits witnessed by another ISMS auditor.

Article	Change
7.2.1.1	The criteria for selecting auditors became stricter. In addition to 7.1.2.1, the criteria for selecting auditors shall ensure that each auditor: a) has professional education or training to an equivalent level of university education; b) has at least four years full time practical workplace experience in information technology, of which at least two years are in a role or function relating to information security; c) has successfully completed at least five days of training, the scope of which covers ISMS audits and audit management; d) has gained experience in the entire process of assessing information security prior to assuming responsibility for performing as an auditor. This experience should have been gained by participation in a minimum of four ISMS certification audits, including re-certification and surveillance audits, for a total of at least 20 days of which at most 5 days may come from surveillance audits. 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. Technical experts shall comply with criteria a), b) and e)
7.2.1.2	The criteria for selecting auditors for leading the team became stricter. In addition to 7.1.2.2 and 7.2.1.1, the criteria for selecting an auditor for leading the team shall ensure that this auditor: a) has actively participated in all stages of at least three ISMS audits. The participation shall include initial scoping and planning, review of documentation and risk assessment, implementation assessment and formal audit reporting.
7.3.1	Technical experts are no longer required to be able to put complex operations in a broad perspective and to understand the role of individual units in larger client organisations. Technical experts shall comply with criteria a), b) and e) of 7.2.1.1
8.4.1	Access to organisational records. It has been clarified what could be understood as 'ISMS related information'; examples are mentioned (such as ISMS records or information about design and effectiveness of controls).
9.1.1.1	New requirement for application readiness: The certification body shall require the client to have a documented and implemented ISMS which conforms to ISO/IEC 27001 and other documents required for certification.
9.1.3.1	Audit programme: The audit programme for ISMS audits shall take the determined information security controls into account.
9.1.3.4	One of the requirements for granting certification has been reworded: the certification body shall not certify an ISMS unless it has been operated through at least one management review and one internal ISMS audit covering the scope of certification.
9.1.3.5	Certification bodies shall ensure that the client's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the scope of certification. Certification bodies shall confirm that this is reflected in the client's scope of their ISMS and Statement of Applicability. The certification body shall verify that there is at least one Statement of Applicability per scope of certification.
9.1.4.1	The calculation of audit time became normative. The certification body shall use Annex B to determine audit time. Remark: the audit time chart in Annex B has an additional entry with regard to the number of persons; the entry 11~ 25 has been split into 11 ~ 15 and 16 ~ 25. The total number of audit days has not changed per entry, except for the above.

Article	Change
9.1.5.1.2	Multiple Site. Additional requirements for sampling of a representative number of sites. It shall additionally take into account: geographical and cultural aspects; risk situation of the sites; information security incidents at the specific sites.
9.2.1.1	New requirement: The audit objectives shall include the determination of the effectiveness of the management system to ensure that the client, based on the risk assessment, has implemented applicable controls and achieved the established information security objectives
9.2.2.2	Audit team competence requirements have been described more clearly.
9.2.3.3	New requirement: A certification body should agree with the organisation to be audited the timing of the audit which will best demonstrate the full scope of the organisation. The consideration could include season, month, day/dates and shift as appropriate.
9.3.1.1	A new requirement for Stage 1 has been added: The certification body shall obtain a sufficient understanding of the design of the ISMS in the context of the client's organisation, risk assessment and treatment (including the controls determined), information security policy and objectives and, in particular, of the client's preparedness for the audit. This allows planning for stage 2.
9.3.1.2.2	There has been an elaboration regarding the focus of the stage 2 audit. The audit shall focus on client's: a) top management leadership and commitment to information security policy and the information security objectives; b) documentation requirements listed in ISO/IEC 27001; c) assessment of information security related risks and that the assessments produce consistent, valid and comparable results if repeated; d) determination of control objectives and controls based on the information security risk assessment and risk treatment processes; e) information security performance and the effectiveness of the ISMS, evaluating against the information security objectives; f) correspondence between the determined controls, the Statement of Applicability and the results of the information security risk assessment and risk treatment process and the information security policy and objectives; g) implementation of controls (see Annex D), taking into account the external and internal context and related risks, the organisation's monitoring, measurement and analysis of information security processes and controls, to determine whether controls are implemented and effective and meet their stated information security objectives; h) programmes, processes, procedures, records, internal audits and reviews of the ISMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives.
9.4.2	Specific elements of the ISMS audit have been more aligned with risks and risk assessments. The certification body, represented by the audit team, shall: a) require the client to demonstrate that the assessment of information security related risks is relevant and adequate for the ISMS operation within the ISMS scope; b) establish whether the client's procedures for the identification, examination and evaluation of information security related risks and the results of their implementation are consistent with the client's policy, objectives and targets. The certification body shall also establish whether the procedures employed in risk assessment are sound and properly implemented.

Article	Change
9.4.3.1	Additional requirement for audit report: In addition to the requirements for reporting in ISO/IEC 17021-1, 9.4.8, the audit report shall provide the following information or a reference to it: a) an account of the audit including a summary of the document review; b) an account of the certification audit of the client's information security risk analysis; c) deviations from the audit plan (e.g. more or less time spent on certain scheduled activities); d) the ISMS' scope.
9.4.3.2	Additional requirement for audit report: The audit report shall be of sufficient detail to facilitate and support the certification decision. It shall contain: a) significant audit trails followed and audit methodologies utilized (see 9.1.3.2); b) observations made, both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities); c) comments on the conformity of the client's ISMS with the certification requirements with a clear statement of nonconformity, a reference to the version of the Statement of Applicability and, where applicable, any useful comparison with the results of previous certification audits of the client.
9.6.2.1.1	Only minor adaptations with regard to surveillance activities.
9.6.2.1.2	New requirements for CABs when conducting a surveillance. As a minimum, every surveillance by the certification body shall review the following: a) the effectiveness of the ISMS with regard to achieving the objectives of the client's information security policy; b) the functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations; c) changes to the controls determined, and resulting changes to the SoA; d) implementation and effectiveness of controls according to the audit programme.
Annex B	This annex on audit time became normative. See 9.1.4.1.