Raad voor Accreditatie (RvA)

Toelichting op de invoering van ISO/IEC 27006:2015

Documentcode:	**RvA-T045-NL**
	Versie 1, 10-10-2016

Een RvA-Toelichting beschrijft het beleid en/of de werkwijze van de RvA met betrekking tot een specifiek accreditatieonderwerp. Indien het beleid en/of de werkwijze betreffende een accreditatieonderwerp, dat in een RvA-Toelichting is beschreven, in een EA, ILAC of IAF-document wordt vastgelegd, zal de RvA haar beleid en werkwijze in overeenstemming brengen met dit EA, ILAC of IAF-document.

Een actuele versie van de Toelichtingen is via de website van de RvA (www.rva.nl) te verkrijgen.

Inhoud

1 Inleiding

Deze toelichting is van toepassing op alle managementsysteemaccreditaties (ISO/IEC 17021-1), met ISO 27001 als scope, die worden beoordeeld met behulp van de ISO/IEC 27006.
Op 1 oktober 2015 is de norm ISO/IEC 27006:2015 “Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems” gepubliceerd. Deze norm vervangt de norm ISO/IEC 27006:2011 met dezelfde titel.
Door het International Accreditation Forum (IAF) is bepaald dat voor de overgang van de ISO/IEC 27006:2011 naar de ISO/IEC 27006:2015 een termijn van 2 jaar wordt gehanteerd, dus tot 1 oktober 2017.
De aanpassingen betreffen allereerst de verwijzingen naar of aanpassingen aan de ISO/IEC 17021-1:2015. Daarnaast betreffen de aanpassingen zowel nieuwe teksten, die nieuwe vereisten toevoegen, als wijzigingen van teksten van ISO/IEC 27006:2011 tot anders geformuleerde vereisten. De aanpassingen met betrekking tot ISO/IEC 17021-1:2015 worden niet apart genoemd, ondanks het feit dat het wijzigingen betreffen op de ISO/IEC 27006:2011 (bijvoorbeeld competentie-eisen).
Deze toelichting beschrijft het RvA-beleid en de RvA-werkwijze met betrekking tot de beoordelingen tegen ISO/IEC 27006:2015, het nemen van besluiten voor accreditatie tegen deze nieuwe norm en het vervangen van de accreditatieverklaringen en scopes van accreditatie.

Na 1 oktober 2017 is accreditatie voor managementsysteemcertificatie voor informatiebeveiliging conform de ISO/IEC 27001:2013 alleen mogelijk indien de instelling een accreditatie conform ISO/IEC 17021-1:2015 bezit en voldoet aan de ISO/IEC 27006:2015-eisen.

2 Overgangsregeling

2.1 Algemeen

De RvA hanteert als uitgangspunt dat de RvA-beoordelingen tegen de nieuwe en gewijzigde vereisten in de nieuwe norm zoveel mogelijk zullen plaatsvinden tijdens de reguliere beoordelingen. De RvA heeft de overgangsbepalingen voor de invoering van de ISO/IEC 27006:2015 hieronder uitgewerkt.

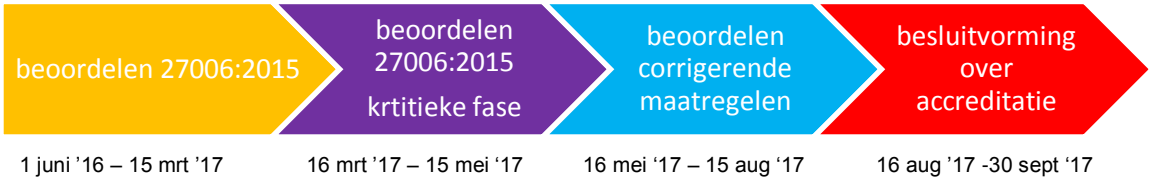
<u>Nieuwe accreditatie-aanvragen:</u>
Voor nieuwe accreditatie-aanvragen wordt vanaf 1 juni 2016 de ISO/IEC 27006:2015 gehanteerd.

<u>Bestaande accreditaties:</u>
1. Bijlage A bevat de vergelijking tussen ISO/IEC 27006:2011 en ISO/IEC 27006:2015. De nieuwe en gewijzigde eisen in ISO/IEC 27006:2015 zijn daarin expliciet benoemd.
2. Vanaf 1 juni 2016 beoordeelt de RvA bij de reguliere beoordelingen tegen eisen uit ISO/IEC 27006:2015. Sectie 2.2 bevat details over de wijze van beoordelen.
3. Voor de afwijkingen die bij beoordelingen tussen 1 juni 2016 en 15 maart 2017 vastgesteld worden tegen nieuwe en/of gewijzigde eisen, die niet als afwijking tegen de eisen uit ISO/IEC 27006:2011 gerapporteerd zouden kunnen worden gelden bijzondere bepalingen voor de

corrigerende maatregelen. Deze bijzondere bepalingen zijn beschreven in sectie 2.3 van deze toelichting.

4. De RvA zal een aangepaste bijlage bij de accreditatieverklaring afgeven nadat vastgesteld is dat aan ISO/IEC 27006:2015 voldaan wordt, daarover een positief besluit genomen is en er een accreditatieverklaring is verstrekt, of tegelijkertijd wordt verstrekt, voor de ISO/IEC 17021-1:2015.
5. Indien dit besluit niet voor 1 oktober 2017 kan worden genomen, wordt het schema betreffende managementsysteemcertificatie voor informatiebeveiliging conform de ISO/IEC 27001:2013 van de bijlage bij de accreditatieverklaring verwijderd.
6. Voor situaties afwijkend van bovenstaande situaties zal de directie van de RvA de werkwijze bepalen.

De tijdlijn voor de transitie is onderstaand schematisch weergegeven.



2.2 RvA-beoordeling van de overgang naar ISO/IEC 27006:2015

De implementatie van de nieuwe en gewijzigde eisen zal de RvA op de volgende wijze beoordelen:

- Met een beoordeling van documenten tijdens en in voorbereiding op de transitiebeoordeling zal het beoordelingsteam verifiëren of de nieuwe en gewijzigde eisen afdoende zijn verwerkt in het gedocumenteerde managementsysteem. Hiertoe zal de instelling een kruisverwijzingslijst tussen de eisen genoemd in Annex A en het eigen gedocumenteerde managementsysteem aan het beoordelingsteam beschikbaar stellen.
- Op basis van de interne audits en management reviews van de instelling zal het beoordelingsteam verifiëren of de instelling zelf de implementatie van de nieuwe en gewijzigde eisen heeft vastgesteld.
- Op basis van dossieronderzoek, interviews en observaties van activiteiten zal het team de implementatie verifiëren.

2.3 Afwijkingen tegen de nieuwe eisen

Afwijkingen tegen de eisen van de ISO/IEC 27006:2015 die geen afwijkingen zouden zijn geweest tegen ISO/IEC 27006:2011 zullen bij beoordelingen die plaatsvinden tussen 1 juni 2016 en 15 maart 2017 gecategoriseerd worden als (B)-afwijkingen. Bijlage A van deze toelichting specificeert tegen welke eisen een (B)-afwijking kan worden geformuleerd. De instelling heeft tot 16 mei 2017 de gelegenheid om corrigerende maatregelen uit te voeren en de rapportage daarover bij de RvA in te dienen (zie RvA-BR004). De RvA zal deze maatregelen beoordelen en het beoordelingsteam zal hierover uiterlijk op 15 augustus 2017 een advies aan de directie van de RvA uitbrengen. De directie van de RvA zal de accreditatiebesluiten nemen voor 1 oktober 2017.

Indien de RvA niet voor 1 oktober 2017 een positief besluit inzake het verlenen van accreditatie voor ISO/IEC 27006:2015 heeft kunnen nemen, als gevolg van het niet kunnen sluiten van de afwijkingen, dan wordt het schema betreffende managementsysteemcertificatie voor informatiebeveiliging conform ISO/IEC 27001:2013 per 1 oktober 2017 van de bijlage bij accreditatieverklaring verwijderd.

3 Wijzigingen ten opzichte van de vorige versie

Geen, dit is de eerste versie van dit toelichtend document.

Bijlage A: Lijst van wijzigingen

Artikel	Wijziging
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.

Artikel	Wijziging
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.

Artikel	Wijziging
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.
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.

Artikel	Wijziging
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.
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.

Artikel	Wijziging
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.