### Inhalt

[5 General requirements 2](#_Toc39045744)

[7 Resource requirements 2](#_Toc39045745)

[8 Information requirements 6](#_Toc39045746)

[9 Process requirements 6](#_Toc39045747)

[10 Management system requirements for certification bodies 13](#_Toc39045748)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Details of the certification body** | | | | |
| Name: |  | | | |
| Address: |  | | | |
| File number: |  |  |  | |
| Case number | Phase |  | |
| Date of assessment: |  | | | |
| Accreditation process: |  | | | |
| Assessment type[[1]](#endnote-1) : |  | | | |
| Certification body with several locations: | | | Yes | No |
| Name / Address of assessed locations: | | | | |

|  |
| --- |
|  |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Details of the assessor** | | | |
| Name: |  | | |
| Status[[2]](#endnote-2) : | SA | TA | TE |
| **Assessed area** (technical fields of DAkkS, certification fields, sector specific requirements, directives/modules) | | | |

|  |
| --- |
|  |

In addition to the report according to DIN EN ISO/IEC 17021-1 this checklist references the detailed requirements of ISO/IEC 27006:2015/Amd.1:2020. **This checklist contains the additional requirements, only - not any pure reference to the accreditation standard itself.**

DAkkS assumes that the reference made within ISO/IEC 27006:2015/Amd.1:2020 toward DIN EN ISO/IEC 17021:2011 applies identically to the relevant clauses of DIN EN ISO/IEC 17021-1:2015. Therefore, further editorial changes were not made.

This checklist / this report does **not** repeat the objective evidence and reviewed documents, text and explanation listed or given in the partial assessment report according to DIN EN ISO/IEC 17021-1:2015. The responsible assessor **may**, however, list further documents and add explanatory text.

# 5 General requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5.2.1 | Certification bodies may carry out the following duties without them being considered as consultancy or having a potential conflict of interest:   1. arranging and participating as a lecturer in training courses, provided that, where these courses relate to information security management, related management systems or auditing, certification bodies shall confine themselves to the provision of generic information and advice which is publicly available, i.e. they shall not provide company-specific advice which contravenes the requirements of b) below; 2. making available or publishing on request information describing the certification body’s interpretation of the requirements of the certification audit standards  (see 9.1.3.6); 3. activities prior to audit, solely aimed at determining readiness for certification audit; however, such activities shall not result in the provision of recommendations or advice that would contravene this clause and the certification body shall be able to confirm that such activities do not contravene these requirements and that they are not used to justify a reduction in the eventual certification audit duration; 4. performing second and third-party audits according to standards or regulations other than those being part of the scope of accreditation; 5. adding value during certification audits and surveillance visits, e.g. by identifying opportunities for improvement, as they become evident during the audit, without recommending specific solutions.   The certification body shall not provide internal information security reviews of the client’s ISMS subject to certification. Furthermore, the certification body shall be independent from the body or bodies (including any individuals) which provide the internal ISMS audit. |  |  |  |  |  |

# 7 Resource requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7.1.1 | The certification body shall ensure that it has knowledge of the technological, legal and regulatory developments relevant to the ISMS of the client which it assesses.  The certification body shall define the competence requirements for each certification function as referenced in Table A.1 of ISO/IEC 17021-1. The certification body shall take into account all the requirements specified in ISO/IEC 17021-1 and 7.1.2 and 7.2.1 of this International Standard that are relevant for the ISMS technical areas as determined by the certification body. |  |  |  |  |  |
| 7.1.2.1.1 | The certification body shall have criteria for verifying the background experience, specific training or briefing of audit team members that ensures at least:   1. knowledge of information security; 2. technical knowledge of the activity to be audited; 3. knowledge of management systems; 4. knowledge of the principles of auditing; 5. 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.  The audit team shall be competent to trace indications of information security incidents in the client’s ISMS back to the appropriate elements of the ISMS.  The audit team shall have appropriate work experience of the items above and practical application of these items (this does not mean that an auditor needs a complete range of experience of all areas of information security, but the audit team as a whole shall have enough appreciation and experience to cover the ISMS scope being audited). |  |  |  |  |  |
| 7.1.2.1.2 | Collectively, all members of the audit team shall have knowledge of:   1. ISMS specific documentation structures, hierarchy and interrelationships; 2. information security management related tools, methods, techniques and their application; 3. information security risk assessment and risk management; 4. processes applicable to ISMS; 5. the current technology where information security may be relevant or an issue. 6. Every auditor shall fulfil a), c) and d). |  |  |  |  |  |
| 7.1.2.1.3 | Auditors involved in ISMS auditing shall have knowledge of:   1. all requirements contained in ISO/IEC 27001.   Collectively, all members of the audit team shall have knowledge of:   1. all controls contained in ISO/IEC 27002 (if determined as necessary also from sector specific standards) and their implementation, categorized as: 2. information security policies; 3. organization of information security; 4. human resource security; 5. asset management; 6. access control, including authorization; 7. cryptography; 8. physical and environmental security; 9. operations security, including IT-services; 10. communications security, including network security management and information transfer; 11. system acquisition, development and maintenance; 12. supplier relationships, including outsourced services; 13. information security incident management; 14. information security aspects of business continuity management, including redundancies; 15. compliance, including information security reviews. |  |  |  |  |  |
| 7.1.2.1.4 | Auditors involved in ISMS auditing shall have knowledge of:   1. industry information security good practices and information security procedures; 2. policies and business requirements for information security; 3. general business management concepts, practices and the inter-relationship between policy, objectives and results; 4. management processes and related terminology. |  |  |  |  |  |
| 7.1.2.1.5 | Auditors involved in ISMS auditing shall have knowledge of:   1. the legal and regulatory requirements in the particular information security field, geography and jurisdiction(s); 2. information security risks related to business sector; 3. generic terminology, processes and technologies related to the client business sector; 4. the relevant business sector practices.   The criteria a) may be shared amongst the audit team. |  |  |  |  |  |
| 7.1.2.1.6 | Collectively, auditors involved in ISMS auditing shall have knowledge of:   1. the impact of organization type, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing; 2. complex operations in a broad perspective; 3. legal and regulatory requirements applicable to the product or service. |  |  |  |  |  |
| 7.1.2.2 | In addition to the requirements in 7.1.2.1, audit team leaders shall fulfil the following requirements, which shall be demonstrated in audits under guidance and supervision:   1. knowledge and skills to manage the certification audit process and the audit team; 2. demonstration of the capability to communicate effectively, both orally and in writing. |  |  |  |  |  |
| 7.1.2.3.1 | 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:   1. relevant ISMS standards and other normative documents used in the certification process. |  |  |  |  |  |
| 7.1.2.3.2 | Personnel conducting the application review to determine the audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of:   1. generic terminology, processes, technologies and risks related to the client business sector. |  |  |  |  |  |
| 7.1.2.3.3 | 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:   1. client products, processes, organization types, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing functions. |  |  |  |  |  |
| 7.1.2.4.1 | The personnel reviewing audit reports and making certification decisions shall have knowledge that enables them to verify the appropriateness of the scope of certification as well as changes to the scope and their impact on the effectiveness of the audit, in particular the continuing validity of the identification of interfaces and dependencies and the associated risks.  Additionally, the personnel reviewing audit reports and making the certification decisions shall have knowledge of:   1. management systems in general; 2. audit processes and procedures; 3. audit principles, practices and techniques. |  |  |  |  |  |
| 7.1.2.4.2 | The personnel reviewing audit reports and making the certification decisions shall have knowledge of:   1. the items listed in 7.1.2.1.2 a), c) and d); 2. legal and regulatory requirements relevant to information security. |  |  |  |  |  |
| 7.1.2.4.3 | Personnel reviewing audit reports and making certification decisions shall have knowledge of:   1. relevant ISMS standards and other normative documents used in the certification process. |  |  |  |  |  |
| 7.1.2.4.4 | Personnel reviewing audit reports and making certification decisions shall have knowledge of:   1. generic terminology and risks related to the relevant business sector practices. |  |  |  |  |  |
| 7.1.2.4.5 | Personnel reviewing audit reports and making certification decisions shall have knowledge of:   1. client products, processes, organization types, size, governance, structure, functions and relationships. |  |  |  |  |  |
| 7.2.1 | The certification body shall demonstrate that the auditors have knowledge and experience through:   1. recognized ISMS-specific qualifications; 2. registration as auditor where applicable; 3. participation in ISMS training courses and attainment of relevant personal credentials; 4. up to date professional development records; 5. ISMS audits witnessed by another ISMS auditor. |  |  |  |  |  |
| 7.2.1.1 | In addition to 7.1.2.1, the criteria for selecting auditors shall ensure that each auditor:   1. has professional education or training to an equivalent level of university education; 2. 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; 3. has successfully completed at least five days of training, the scope of which covers ISMS audits and audit management; 4. has gained experience of auditing ISMS prior to acting as an auditor performing ISMS audits. This experience shall be gained by performing as an auditor-in-training monitored by an ISMS evaluator  (see ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one  ISMS initial certification audit (stage 1 and stage 2) or  re-certification and at least one surveillance audit. This experience shall be gained in at least 10 ISMS on-site audit days and performed in the last 5 years. The partici­pation shall include review of documentation and risk assessment, implementation assessment and audit reporting. 5. has relevant and current experience; 6. keeps current knowledge and skills in information security and auditing up to date through continual professional development. 7. has competence in auditing an ISMS in accordance with ISO/IEC 27001.   Technical experts shall comply with criteria a), b) and e). |  |  |  |  |  |
| 7.2.1.2 | 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:   1. 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 shall work under the supervision of an auditor. The minimum requirements for technical experts are listed in 7.2.1.1. |  |  |  |  |  |

# 8 Information requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 8.2.1 | Certification documents shall be signed by an officer who has been assigned such responsibility. The version of the Statement of Applicability shall be included in the certification documents.  The certification documents may reference national and international standards as source(s) of control set for controls that are determined as necessary in the organization's Statement of Applicability in accordance with ISO/IEC 27001:2013, 6.1.3 d). The reference on the certification documents shall be clearly stated as being only a control set source for controls applied in the Statement of Applicability and not a certification thereof. |  |  |  |  |  |
| 8.4.1 | Before the certification audit, the certification body shall ask the client to report if any ISMS related information (such as ISMS records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information. The certification body shall determine whether the ISMS can be adequately audited in the absence of such information. If the certification body concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, it shall advise the client that the certification audit cannot take place until appropriate access arrangements are granted. |  |  |  |  |  |

# 9 Process requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 9.1.1.1 | 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 | The audit programme for ISMS audits shall take the determined information security controls into account. |  |  |  |  |  |
| 9.1.3.2 | The certification body’s procedures shall not presuppose a particular manner of implementation of an ISMS or a particular format for documentation and records. Certification procedures shall focus on establishing that a client’s ISMS meets the requirements specified in ISO/IEC 27001 and the policies and objectives of the client. |  |  |  |  |  |
| 9.1.3.3 | The certification body shall require that a client makes all necessary arrangements for the access to internal audit reports and reports of independent reviews of information security.  At least the following information shall be provided by the client during stage 1 of the certification audit:   1. general information concerning the ISMS and the activities it covers; 2. a copy of the required ISMS documentation specified in ISO/IEC 27001 and, where required, associated documentation. |  |  |  |  |  |
| 9.1.3.4 | 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 | The audit team shall audit the ISMS of the client covered by the defined scope against all applicable certification requirements. The certification body shall confirm, in the scope of the client ISMS, that clients address the requirements stated in ISO/IEC 27001, 4.3.  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.  Certification bodies shall ensure that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS subject to certification and are included in the client’s information security risk assessment. An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organizations. |  |  |  |  |  |
| 9.1.3.6 | The criteria against which the ISMS of a client is audited shall be the ISMS standard ISO/IEC 27001. Other documents may be required for certification relevant to the function performed. |  |  |  |  |  |
| 9.1.4.1 | Certification bodies shall allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or re-certification audit. The calculation of overall audit time shall include sufficient time for audit reporting. |  |  |  |  |  |
| 9.1.5.1.1 | Where a client has a number of sites meeting the criteria from a) to c) below, certification bodies may consider using a sample-based approach to multiple-site certification audit:   1. all sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review; 2. all sites are included within the client’s internal ISMS audit programme; 3. all sites are included within the client’s ISMS management review programme. |  |  |  |  |  |
| 9.1.5.1.2 | The certification body wishing to use a sample-based approach shall have procedures in place to ensure the following:   1. The initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined. 2. A representative number of sites have been sampled by the certification body, taking into account:    1. the results of internal audits of the head office  and the sites;    2. the results of management review;    3. variations in the size of the sites;    4. variations in the business purpose of the sites;    5. complexity of the information systems  at the different sites;    6. variations in working practices;    7. variations in activities undertaken;    8. variations of design and operation of controls;    9. potential interaction with critical information  systems or information systems processing  sensitive information;    10. any differing legal requirements;    11. geographical and cultural aspects;    12. risk situation of the sites;    13. information security incidents at the specific sites. 3. A representative sample is selected from all sites within the scope of the client’s ISMS; this selection shall be based upon judgmental choice to reflect the factors presented in item b) above as well as a random element. 4. Every site included in the ISMS which is subject to significant risks is audited by the certification body prior to certification. 5. The audit programme has been designed in the light of the above requirements and covers representative samples of the scope of the ISMS certification within the three year period. 6. In the case of a nonconformity being observed, either at the head office or at a single site, the corrective action procedure applies to the head office and all sites covered by the certificate.   The audit shall address the client’s head office activities to ensure that a single ISMS applies to all sites and delivers central management at the operational level. The audit shall address all the issues outlined above. |  |  |  |  |  |
| 9.1.6.1 | The certification body may accept documentation that is combined (e.g. for information security, quality, health and safety and environment) as long as the ISMS can be clearly identified together with the appropriate interfaces to the other systems. |  |  |  |  |  |
| 9.1.6.2 | The ISMS audit may be combined with audits of other management systems, provided that it can be demonstrated that the audit satisfies all requirements for certification of the ISMS. All the elements important to an ISMS shall appear clearly and be readily identifiable in the audit reports. The quality of the audit shall not be adversely affected by the combination of the audits. |  |  |  |  |  |
| 9.2.1.1 | 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. |  |  |  |  |  |
| 9.2.2.1 | The audit team shall be formally appointed and provided with the appropriate working documents. The mandate given to the audit team shall be clearly defined and made known to the client.  An audit team may consist of one person provided that the person meets all the criteria set out in 7.1.2.1. |  |  |  |  |  |
| 9.2.2.2 | The requirements listed in 7.1.2 apply. For surveillance and special audit activities, only those requirements which are relevant to the scheduled surveillance activity and special audit activity apply.  When selecting and managing the audit team to be appointed for a specific certification audit the certification body shall ensure that the competences brought to each assignment are appropriate.  The team shall:   1. have appropriate technical knowledge of the specific activities within the scope of the ISMS for which certification is sought and, where relevant, with associated procedures and their potential information security risks (technical experts may fulfil this function); 2. have understanding of the client sufficient to conduct a reliable certification audit of its ISMS given the ISMS’ scope and context within the organization in managing the information security aspects of its activities, products and services; 3. have appropriate understanding of the legal and regulatory requirements applicable to the client’s ISMS. |  |  |  |  |  |
| 9.2.3.1 | The audit plan for ISMS audits shall take the determined information security controls into account. |  |  |  |  |  |
| 9.2.3.2 | The audit plan shall identify the network-assisted auditing techniques that will be utilized during the audit, as appropriate.  Network assisted auditing techniques may include, for example, teleconferencing, web meeting, interactive web-based communications and remote electronic access to the ISMS documentation or ISMS processes. The focus of such techniques should be to enhance audit effectiveness and efficiency and should support the integrity of the audit process. |  |  |  |  |  |
| 9.2.3.3 | A certification body should agree with the organization to be audited the timing of the audit which will best demonstrate the full scope of the organization. The consideration could include season, month, day/dates and shift as appropriate. |  |  |  |  |  |
| 9.3.1.1 | In the stage 1 of the audit the certification body shall obtain documentation on the design of the ISMS covering the documentation required in ISO/IEC 27001.  The certification body shall obtain a sufficient understanding of the design of the ISMS in the context of the client’s organization, 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.  The results of stage 1 shall be documented in a written report. 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; this may be done by the auditor leading the team that conducted the stage 1 audit if deemed competent and appropriate.  NOTE Independent review (i.e. by a person from the certification body not involved in the audit) is one measure to mitigate the risks involved when deciding if and with whom to proceed to stage 2. However, other risk mitigation measures can already be in place achieving the same goal.  The certification body shall make the client aware of the further types of information and records that may be required for detailed examination during stage 2. |  |  |  |  |  |
| 9.3.1.2.1 | On the basis of findings documented in the stage 1 audit report, the certification body develops an audit plan for the conduct of stage 2. In addition to evaluating the effective implementation of the ISMS, the objectives of stage 2 are:   1. to confirm that the client adheres to its own policies, objectives and procedures. |  |  |  |  |  |
| 9.3.1.2.2 | To do this, the audit shall focus on the client’s:   1. top management leadership and commitment to information security policy and the information security objectives; 2. documentation requirements listed in ISO/IEC 27001; 3. assessment of information security related risks and that the assessments produce consistent, valid and comparable results if repeated; 4. determination of control objectives and controls based on the information security risk assessment and risk treatment processes; 5. information security performance and the effectiveness of the ISMS, evaluating against the information security objectives; 6. 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; 7. implementation of controls (see Annex D), taking into account the external and internal context and related risks, the organization’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; 8. 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. |  |  |  |  |  |
| 9.4.1 | The certification body shall have documented procedures for:   1. the initial certification audit of a client’s ISMS, in accordance with the provisions of ISO/IEC 17021-1; 2. surveillance and re-certification audits of a client’s ISMS in accordance with ISO/IEC 17021-1 on a periodic basis for continuing conformity with relevant requirements and for verifying and recording that a client takes corrective action on a timely basis to correct all nonconformities. |  |  |  |  |  |
| 9.4.2 | The certification body, represented by the audit team, shall:   1. 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; 2. 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 | 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:   1. an account of the audit including a summary of the document review; 2. an account of the certification audit of the client’s information security risk analysis; 3. deviations from the audit plan (e.g. more or less time spent on certain scheduled activities); 4. the ISMS’ scope. |  |  |  |  |  |
| 9.4.3.2 | The audit report shall be of sufficient detail to facilitate and support the certification decision. It shall contain:   1. significant audit trails followed and audit methodologies utilized (see 9.1.3.2); 2. observations made, both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities); 3. 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.   Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the audit report. If these methods are used, these documents shall be submitted to the certification body as evidence to support the certification decision. Information about the samples evaluated during the audit shall be included in the audit report, or in other certification documentation.  The report shall consider the adequacy of the internal organization and procedures adopted by the client to give confidence in the ISMS.  In addition to the requirements for reporting in ISO/IEC 17021-1, 9.4.8, the report shall cover:  — a summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS requirements and IS controls;  — the audit team’s recommendation as to whether the client’s ISMS should be certified or not, with information to substantiate this recommendation. |  |  |  |  |  |
| 9.5.1 | The certification decision shall be based, additionally to the requirements of ISO/IEC 17021-1, on the certification recommendation of the audit team as provided in their certification audit report (see 9.4.3).  The persons or committees that take the decision on granting certification should not normally overturn a negative recommendation of the audit team. If such a situation does arise, the certification body shall document and justify the basis for the decision to overturn the recommendation.  Certification shall not be granted to the client until there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective and will be maintained. |  |  |  |  |  |
| 9.6.2.1.1 | Surveillance audit procedures shall be consistent with those concerning the certification audit of the client’s ISMS as described in this International Standard.  The purpose of surveillance is to verify that the approved ISMS continues to be implemented, to consider the implications of changes to that system initiated as a result of changes in the client’s operation and to confirm continued compliance with certification requirements. Surveillance audit programmes shall cover at least:   1. the system maintenance elements such as information security risk assessment and control maintenance, internal ISMS audit, management review and corrective action; 2. communications from external parties as required by the ISMS standard ISO/IEC 27001 and other documents required for certification; 3. changes to the documented system; 4. areas subject to change; 5. selected requirements of ISO/IEC 27001; 6. other selected areas as appropriate. |  |  |  |  |  |
| 9.6.2.1.2 | As a minimum, every surveillance by the certification body shall review the following:   1. the effectiveness of the ISMS with regard to achieving the objectives of the client’s information security policy; 2. the functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations; 3. changes to the controls determined, and resulting changes to the SoA; 4. implementation and effectiveness of controls according to the audit programme. |  |  |  |  |  |
| 9.6.2.1.3 | The certification body shall be able to adapt its surveillance programme to the information security issues related to risks and impacts on the client and justify this programme.  Surveillance audits may be combined with audits of other management systems. The reporting shall clearly indicate the aspects relevant to each management system.  During surveillance audits, certification bodies shall check the records of appeals and complaints brought before the certification body and, where any nonconformity or failure to meet the requirements of certification is revealed, that the client has investigated its own ISMS and procedures and taken appropriate corrective action.  A surveillance report shall contain, in particular, information on clearing of nonconformities revealed previously and the version of the SoA and important changes from the previous audit. As a minimum, the reports arising from surveillance shall build up to cover in totality the requirements of 9.6.2.1.1 and 9.6.2.1.2 above. |  |  |  |  |  |
| 9.3.6.1 | Re-certification audit procedures shall be consistent with those concerning the initial certification audit of the client’s ISMS as described in this International Standard.  The time allowed to implement corrective action shall be consistent with the severity of the nonconformity and the associated information security risk. |  |  |  |  |  |
| 9.6.4.1 | The activities necessary to perform special audits shall be subject to special provision if a client with a certified ISMS makes major modifications to its system or if other changes take place which could affect the basis of its certification. |  |  |  |  |  |
| 9.8.1 | Complaints represent a potential incident and an indication to possible nonconformity. |  |  |  |  |  |

# 10 Management system requirements for certification bodies

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 10.1.1 | It is recommended that certification bodies implement an ISMS in accordance with ISO/IEC 27001. |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Report was prepared as an annex to the report in accordance with EN ISO/IEC 17021-1:**[[3]](#endnote-3) | | | | | |
| Place: |  | Date: |  | Signed *Name assessor:* | [[4]](#endnote-4) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Report reviewed by the customer manager:** | | | | | |
| Place: |  | Date: |  | Signed *case manager:* |  |

Notes:

\* Grading of fulfilment the requirements of a section of the standard to be entered by the assessor:

1 **No** non-conformity

2 **Non critical** non-conformity

3 **Critical** non-conformity

\*\* Reference to the non-conformity described in the main report (No. of non-conformity there)

1. Under assessment type, the assessment technique is to be indicated, whereby several assessment types can be used in the context of an assessment. Please select the applicable element or combination of elements from the following options to indicate the type of assessment:   
   On-site assessment / Remote assessment / Witness audit (on-site) / Witness audit (remote) / Witness examination / Document review / Other assessment activity (please specify if necessary) [↑](#endnote-ref-1)
2. Status in the assessment team: SA=System Assessor; TA=Technical Assessor; TE=Technical expert [↑](#endnote-ref-2)
3. The assessment of fulfilment the requirements and recommendations for accreditation are documented in the assessment report to the EN ISO/IEC 17021-1. [↑](#endnote-ref-3)
4. This report was prepared personally by on . [↑](#endnote-ref-4)