A50VA02

Spezifische Anforderungen zur Zertifizierung von InfMS (ISMS, BCMS, SMS)
Specific requirements for management system certification InfMS (ISMS, BCMS, SMS)

TÜV NORD Zertifizierung

Inhalt Seite

1 Zweck ... 3
2 Geltungsbereich ... 3
3 Definitionen ... 3
4 Zuständigkeiten ... 4
4.1 Zertifizierungsstellenleiter / Fachleiter ... 4
4.2 Außenstellen ... 4
4.3 Auditoren ... 4
4.4 Fachexperten, Übersetzer, Dolmetscher, Beobachter und Auditoren in Ausbildung ... 4
4.5 Services (Inland, Ausland: unselbständige Außenstellen) ... 4
4.6 Auditorenkompetenz ... 4
5 Ablaufbeschreibung ... 4
5.1 Kundenanfrage / Angebotserstellung ... 5
5.2 Auditdurchführung ... 7
5.3 Zertifikaterteilung und Überwachung ... 15
5.4 Zertifizierung von Unternehmen mit mehreren Standorten ... 19
5.5 Aussetzung, Zurückziehen, Wiederherstellung, Erneuerung, Verweigerung, Kündigung und Einschränkung des Geltungsbereichs von Zertifikaten ... 19
5.6 Kalkulation kombinierter Verfahren InfMS und QMS ... 19
6 Anlagen ... 19
6.1 Ablaufschema Zertifizierungsperiode (A00F284) ... 19

Table of Contents Page

1 Purpose ... 3
2 Area of application ... 3
3 Definitions ... 3
4 Responsibilities ... 4
4.1 Head of Certification Body and Specialist Manager ... 4
4.2 Branch Offices ... 4
4.3 Auditors ... 4
4.4 Technical experts, translators, interpreters, observers and auditors-in-training ... 4
4.5 Services (Germany, other countries: non-critical branch offices) ... 4
4.6 Auditor Competence ... 4
5 Process Description ... 4
5.1 Client inquiry / drafting of offer ... 5
5.2 Audit execution ... 7
5.3 Certificate Issue and Surveillance ... 15
5.4 Multi-site certification ... 19
5.5 Suspension, withdrawal, restoring, renewing, refusing, cancellation and limitation of the scope of certificates ... 19
5.6 Calculation of combined procedures and QMS ... 19
6 Appendices ... 19
6.1 Flowsheet Certification period (A00F284e) ... 19

Dieses Dokument wurde gemäß CERT-401-VA-007 freigegeben. Details zur Freigabe sind von der QM-Stelle verfügbar.
This document has been approved according to CERT-401-VA-007. Details are available from the QM-Department.

7 Mitgeltende Unterlagen 19

7 Other relevant documents..... 19

As in previous version German translation is available only for some parts and will be completed as required.

1 Zweck

Die Anforderungen aus der [A00VA02] gelten

In Ergänzung:
Die Anweisung [A50VA02] beschreibt die zusätzlichen besonderen Anforderungen, die bei Audit und Zertifizierung von InfMS (namentlich BCMS, ISMS und SMS) anzuwenden sind.

Zur Verbesserung der Lesbarkeit werden die Namen von Standards in der Regel vereinfacht, z.B. anstatt DIN EN ISO/IEC 27001 wird dafür die ISO 27001 verwendet.

Im Fall von Widersprüchen zwischen diesem Dokument und der grundlegenden allgemeinen Anweisung müssen die Vorgaben dieses Dokuments angewendet werden.

2 Geltungsbereich

Diese Anweisung gilt für die TÜV NORD CERT GmbH (TN CERT) sowie für alle internationalen Vorgänge, bei denen Akkreditierungen, Zulassungen, Benennungen etc. der TN CERT GmbH genutzt bzw. Dienstleistungen der TN CERT GmbH erbracht werden.

3 Definitionen

Definitionen aus [A00VA02] gelten

BCMS Business Continuity Management System; z.B. aus ISO 22301

ISMS Information Security Management System, z.B. aus ISO 27001

SMS Service Management System, z.B. aus ISO 20000-1

Kunde:
Organisation, deren Managementsysten auditiert und zertifiziert werden soll (ISO 17021-1:2015 3.5)

1 Purpose

The requirements from [A00VA02] apply

Additionally:
Procedure [A50VA02] describes the additional specific requirements which apply for audit and certification for InfMS (namely BCMS, ISMS, SMS).

To improve readability the names of standards are typically simplified, i.e. instead of DIN EN ISO/IEC 27001 the form ISO 27001 will be used.

In the case of contradictions between this document and basic generic procedure, these specific procedure shall be applied.

2 Area of application

This document applies for TÜV NORD CERT GmbH (TN CERT) as well as all international proceedings which make use of TN CERT GmbH accreditations, approvals, notifications etc. and/or when delivering TN CERT GmbH services.

3 Definitions

Defintions from [A00VA02] apply

BCMS Business Continuity Management System; e.g. ISO 22301

ISMS Information Security Management System, e.g. ISO 27001

SMS Service Management System, e.g. ISO 20000-1

Client:
Organization whose management system is being audited for certification purposes (ISO 17021-1:2015 3.5)

Zertifizierter Kunde:
Organisation, deren Managementsystem zertifiziert wurde
(ISO 17021-1:2015 3.1)

Auftraggeber:
Auftraggeber eines zertifizierten Kunden

4 Zuständigkeiten

4.1 Zertifizierungsstellenleiter / Fachleiter

[A00VA02] gilt

4.2 Außenstellen

[A00VA02] gilt

4.3 Auditoren

[A00VA02] gilt

4.4 Fachexperten, Übersetzer, Dolmetscher, Beobachter und Auditoren in Ausbildung

[A00VA02] gilt

4.5 Services (Inland, Ausland: unselbständige Außenstellen)

[A00VA02] gilt

4.6 Auditorenkompetenz

[A00VA02] gilt

5 Ablaufbeschreibung

[A00VA02] gilt

Certified client:
Organization whose management system has been certified
(ISO 17021-1:2015 3.1)

Customer:
Customer of a certified client

4 Responsibilities

4.1 Head of Certification Body and Specialist Manager

[A00VA02] applies

4.2 Branch Offices

[A00VA02] applies

4.3 Auditors

[A00VA02] applies

4.4 Technical experts, translators, interpreters, observers and auditors-in-training

[A00VA02] applies

4.5 Services (Germany, other countries: non-critical branch offices)

[A00VA02] applies

4.6 Auditor Competence

[A00VA02] applies

5 Process Description

[A00VA02] applies

5.1 Kundenanfrage / Angebotserstellung

[A00VA02] gilt

Ergänzend gilt:

Für Anfragen zu InfMS werden anstatt oder zusätzlich zu den generischen einige spezifische Werkzeuge und Vorlagen genutzt.

- [A00F100 Anlage ISO27001] als zusätzlicher Kundenfragebogen
- [A00F100 Anlage ISO27001 Multisite] als zusätzlicher Kundenfragebogen für (komplexe) Multisite-Zertifizierungen;
  Anmerkung: Dieser Fragebogen dient dazu, bereits in der Angebotsphase zusätzlich zur Abfrage der zugrundeliegenden Organisationsstruktur (u.a. Standorte inkl. Klassifizierung, Legaleinheiten, Mitarbeiterzahlen, standortspezifische Geltungsbereiche) auch schon die resultierende Zertifikatsstruktur mit dem Kunden abzustimmen.
- [A50F011] als anzuwendendes Kalkulationstool

Documents and/or form sheets

Policies, procedures, work instructions and form sheets (as applicable) for audit and certification activities in IT related services shall be provided in German and English language.

As long as editions in German language are not available, the edition in English language shall be used.

5.1 Client inquiry / drafting of offer

[A00VA02] applies

Additionally:

For InfMS inquiries some specific tools and templates are used additionally or instead of generic ones

- [A00F100 Anlage ISO27001e] as additional questionnaire
- [A00F100 Anlage ISO27001 Multisite] as additional questionnaire for (complex) multisite certifications;
  Note: This questionnaire serves to coordinate the resulting certificate structure with the client in the offer phase already in addition to the inquiry of the underlying organizational structure (e.g. locations incl. classification, legal units, number of employees, location-specific scopes).
- [A50F011] as applicable calculation tool

Any calculator prepares the audit program (calculation of audit times and duration) using calculation tool and reviewing input information. If not performed by a nominated calculator, an approval by a nominated calculator is required. Appointment as a lead auditor for appropriate standads as well as specialist management or CSM IT includes competence as nominated calculator.

For ISMS (ISO 27001) some modifications shall be applied as follows

5.1.1 Organization

Following ISO/IEC JTC 1/SC 27 clarification document “LIAISON RESPONSE TO ISO/CASCO CLARIFICATION REQUEST FORM (QS-CAS-PROC/31)” [ISO/IEC JTC 1/SC 27 N18613] a client is not necessarily to be a (single) legal entity but can be any kind of organization as defined in ISO 27000.

Therefore, depending on the scope statement this could lead to an organization that can be a part of a company. Any organization shall clearly demonstrate to be a person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives as defined in DAkkS Resolution 4/2017 published in DAkkS document “71 SD 6 039, Revision 1.8, 29.06.2019” [DAkkS Resolution 4/2017].

In these cases, the management system shall clearly demonstrate scope, structure, boundaries and limitations.

The name of organization shall be used in a manner to avoid any misunderstanding about the certified organisation in comparison to any other entity with similar names or addresses, i.e. to add names of divisions/departments etc. to clearly demonstrate boundaries and limitations.

Following [DAkkS Resolution 4/2017] it is not accepted that an organization can be certified following the objective to develop/design, implelemt/establish, operate, monitor, maintain or improve a (information security) management system.

5.1.2 Personnel to be taken into account

ISO 27006 as well as clarification [ISO/IEC JTC 1/SC 27 N18613] define the total number of persons doing work under the organization’s control for all shifts within the scope of ISMS and certification as the the starting point for determination of audit time. Therefore as well external staff (from point of view out of organization as defined above) shall be taken into account if working under the organization’s control.

5.1.3 Access to organizational records

If the client reports, that any ISMS or SMS related information (such as ISMS/SMS records or information about design and effectiveness of controls or services) cannot be made available for review by the audit team because it contains confidential or sensitive information, the specialist management shall determine, whether the ISMS/SMS can be adequately audited in the absence of such information. If the conclusion is, that it is not possible to adequately audit the ISMS/SMS without reviewing the identified confidential or sensitive information, the client shall be advised that the certification audit cannot take place until appropriate access arrangements are granted.

5.1.4 On site audit duration

Differing from general IAF requirements ISO 27006 requires to use at least 70% of determined audit time as on site audit duration. Travelling times (as well between sites), times spend by (technical) experts, auditors in training or other observers are not calculated as audit time.

For audit duration of BCMS or SMS the general rule to use at least 80% of determined audit time as on site audit duration is applied.

Calculation tool [A50F011] applies the described approach.

5.2 Auditdurchführung

5.2 Audit execution

5.2.1 Audit Preparation

[A00VA02] applies

For ISMS and BCMS the audit team shall have adequate technical competence if required competence level corresponding to technical area of scope of organization is determined to be “high” according to [A50VA01Ae]. In these cases, at least one member of the team shall demonstrate necessary competence for corresponding technical area to be an appointed auditor or technical expert for QMS (ISO 9001 etc) or EMS (ISO 14001 or ISO 50001), at which the EAC/TA appointment information of the auditor/expert shall be documented in the ATEA spreadsheet of [A50F011_ACE].

When splitting the audit team, it shall be ensured that the overall competence of the audit team is in place to achieve objectives of the audit.

Working times of technical experts not acting as auditors shall not be considered as “audit time”.

5.2.2 Stage 1 Audit

[A00VA02] applies

Lead auditor shall report results of stage 1 audit in [A00F204] and shall decide representing the certification body how stage 2 shall be continued (audit team, audit time, duration and site samples).

If lead auditor identifies any necessary modification for audit program, these aspects shall be cleared in cooperation with responsible Service unit which will bring in specialist management as necessary.

Audit team shall record results of review of documented information, particularly management system documentation (“manual”) in corresponding standard specific form sheets (A49F221/ A50F221/ A79F221).

5.2.3 Audit planning (Stage 2)

[A00VA02] applies

As appropriate, the audit plan shall identify remote sessions and the remote auditing techniques that will be utilized during the audit. Remote auditing techniques shall not represent more than 30% of the planned on-site audit time.

On the basis of findings documented in stage 1 audit report or in the audit report from the last audit, the audit team shall evaluate the effective implementation of the MS and the objectives of audits on site are to confirm that the client adheres to its own policies, objectives and procedures.

For BCMS

The audit shall focus on the client organization's

a) assessment of information security related risks, and that the assessments produce comparable and reproducible results;
b) BCMS system documentation, see 5.2.1 audit stage 1
c) selection of Business continuity plans/ Incident management plans based on the business impact analysis and risk assessment;
d) reviews of the effectiveness of the BCMS and measurements of the effectiveness of the reporting and reviewing against the BCM objectives;
e) internal BCM audits and management reviews;
f) management responsibility for the BCM policy;
g) correspondence between the business impact analysis, incident response structure and the business continuity plans and the BCM policy and objectives;
h) programmes, processes, procedures, records, internal audits, and reviews of the BCMS effectiveness to ensure that these are traceable to management decisions and the BCM policy and objectives

For ISMS

The audit shall focus on the client organization's

a) top management leadership and commitment to information security policy and the information security objectives;
b) documentation requirements listed in ISO 27001;
c) assessments 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, evaluation 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 of ISO 27006:2015), taking into account the external and internal context 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; programs, processes, procedures, records, internal audits and reviews of ISMS effectiveness to ensure that these are traceable to top management decisions and information security policy and objectives.

For SMS

The audit shall focus on the client organization's

a) assessment of information security related risks, and that the assessments produce comparable and reproducible results;
b) SMS system documentation, see 5.2.1 audit stage 1
c) traceability of processes for fulfilment the overall service delivery processes
d) interfaces and interactions of the processes which are defined in the areas
a) service delivery processes
b) relationship processes
c) resolution processes
d) control processes
e) release processes

5.2.4 Stage 2 Audit

[A00VA02] applies

In Addition

For BCMS

The audit shall focus on the client organization's

a) assessment of information security related risks, and that the assessments produce comparable and reproducible results;

b) BCMS system documentation, see 5.2.1 audit stage 1
c) selection of business continuity plans/ Incident management plans based on the business impact analysis and risk assessment;
d) reviews of the effectiveness of the BCMS and measurements of the effectiveness of the report-ing and reviewing against the BCM objectives;
e) internal BCM audits and management reviews;
f) management responsibility for the BCM policy;
g) correspondence between the business impact analysis, incident response structure and the business continuity plans and the BCM policy and objectives;
h) programmes, processes, procedures, records, internal audits, and reviews of the BCMS effec-tiveness to ensure that these are traceable to management decisions and the BCM policy and objectives.

For ISMS

Considering the results of stage 1 or previos audits the audit team shall evaluate the effective implementation of the ISMS to confirm that the client adheres to its own policies, objectives and procedures.

To do this, the audit shall focus on the client's:

a) top management leadership and commit-ment to information security policy and the information security objectives;
b) documentation requirements listed in ISO 27001;
c) assessments 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, evaluation 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 of ISO 27006:2015), taking into account the external and internal context 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; programs, processes, procedures, records, internal audits and reviews of ISMS effec-tiveness to ensure that these are traceable to top management decisions and information security policy and objectives.

For SMS

The audit shall focus on the client organization's

a) assessment of information security related risks, and that the assessments produce comparable and reproducible results;
b) SMS system documentation, see 5.2.1 audit stage 1
c) traceability of processes for fulfilment the overall service delivery processes
d) interfaces and interactions of the processes which are defined in the areas
a) service delivery processes
b) relationship processes
c) resolution processes
d) control processes
e) release processes

5.2.5 Audit Findings/Documentation of the audit

[A00VA02] applies

Some audit file documents are required to be InfMS specific edition as described here.

General:

The audit documentation shall be provided at least in German or English language, files in other languages are accepted only in addition.

All audit files should be provided as PDF files.

Mandatory for any ISMS audit (ISO 27001): [A50F207e - Supplemental Report ISMS]

Lead auditor shall prepare this document.

Details of sope and SoA (Statement of Applicability) shall be recorded here - mandatory for ISMS/ISO 27001 especially the identification of revision/edition and issue date.

The scope of certificate shall be consistent to scope of the ISMS and the corresponding text in audit report and shall reflect the objectives of the organization in conjuction to relevant core processes and/or products/services.
Note: The term “ISMS” is unwelcome in scope text.

If relevant modification of the SoA changing the coverage of controls is determined in the audit, the lead auditor shall initate reissuance of modified certificate using this report.

Any exclusion or comment on applicability of controls in the SoA shall be recorded in corresponding table in this document.

Mandatory for any InfMS audit: [A50F212e - Session Summary]

Replacing or in addition to handwritten notes any auditor (auditors and lead auditor) in an InfMS audit shall record a brief summary in English or German language of every audit session he/she participated.

[**A50F212e**] shall be used to log the results of each audit session briefly corresponding to requirements being identified at least as reference to 2nd level of clause numbers of audited standards.

[**A50F212e**] is an internal working document and shall not be used for any common or client purpose.

In addition to [A00F207e - Audit report-2] and [**A50F212e**] the auditor can have prepared handwritten notes and/or collected client screenshots or other evi-

dence like client documents or records. These objective evidences shall be archived confidentially by the audit team and provided to veto person on request. They shall be deleted after having received final approval in veto process.

Evidences should be collected by the auditor during the audit sessions. These evidences should be archived for at least four years by the client.

Note: It is a good practice to declare statements with "NCA", "NCB", "PI", "GP" or "CM" if they are the sources for statements in the [A00F207e - Audit report-2].

Note: Related session evidence should be declared with [ ] brackets or hyperlinks.

Note: Internal Comments from the auditor should be redcorded in { } brackets.

[A00F206e - Audit plan-2]

The standard requirement references should record at least the 2nd level of the clauses in [A00F206e - Audit plan-2].

Examples:

- ISO 27001 chapter 8.1, short "8.1" for "Operational planning and control"

or

- ISO 27001 Annex A.6.1, short "A.6.1" for "Internal organization".

In some special cases some more information as provided in the [A00F206e - Audit plan-2] table could be seen as necessary. In this cases the audit team leader may generate an own audit plan table in the form of an annex having at least the same attributes as table in [A00F206e - Audit plan-2] but may contain additional columns like "audit session duration", "documented information" or "sum". An example for this annex is given by [A50F206A01e - Audit-plan-2 Annex]

[A00F207e - Audit report-2]

If any difference exists between the findings listed in [A00F207e - Audit report-2] and [A50F212e - Session Summary], the [A00F207e - Audit report-2] is the leading and binding document.

If an audit results in status “non-conform” this shall be recorded in the tables for “non-conformity” only and not in any other tables of the [A00F204e - Audit report-1] or [A00F207e - Audit report-2].

Any non-conformity shall contain the term “SHALL” (or “SHALL NOT”) in its non-conformity statement.

Strongly recommended: [A50F252e - Annex to Release Protocol]

Annex to Release Protocol supports veto process in both phases and improves communication between audit team and veto staff. Any other valid method is accepted as well.

5.3 Zertifikaterteilung und Überwachung

5.3 Certificate Issue and Surveillance

5.3.1 Certificate issue

[A00VA02] applies

In addition/modification:
Veto process is performed in two stages, maybe by different persons.
In veto 1 only formal aspects are reviewed like completeness of file, correctness of application and use of formsheets or documents. This may be performed by any staff appointed for veto 1, but as well by appointed veto 2 staff.
In veto 2 the content of documents is reviewed to understand the integrity of the audit to get to final decision on certification. That shall be performed by appointed veto 2 persons only.

It is recommended to use [A50F252e] to record details of veto process in any iteration. This form sheet may be updated or re-issued in any iteration of veto process until final decision. It should be uploaded into workflow as WORD-file to support application until final decision. Final version after final decision should be uploaded as PDF-file.
At least [A00F251] shall be used to record final decision at the end of veto 2.

For BCMS audits: Veto 2 person for BCMS audits shall have knowledge of the context in which the organization operates.

In the case, veto 2 person – always acting on behalf of certification body – intends to overturn the recommendation of audit team, the decision shall be justified and recorded in the [A00F251].

Veto 2 persons are acting on behalf of certification body and their activities are not limited to audits performed in the own region. To gain and keep sufficient experience in veto reviews, it is necessary for veto staff to perform veto reviews regularly.

For ISMS: SoA and Additional Standards as source of controls
SoA shall be referred correctly in addition to certification scope for ISO 27001 as defined in template for certificate.
ISO 27006 allows to refer to additional national or international standards in certification documents for ISO 27001 certification. [A50VA06] defines the conditions and processes how to implement, maintain, update and discontinue services for such standards.
If additional standards were used by client as source of controls, listed correctly in SoA and audited during the audit correctly, the certificate shall contain an addition to scope text referring to these standards as defined in template for certificate.
If SoA is modified relevant to certification scope after issuance of certificate, a revised certificate shall be re-issued.

Addition to certification scope in template for ISO 27001:
*"**As per the Statement of Applicability of <dd.mm.yyyy> (version <XY>)***
{optional:} referring to applicable controls defined in standard(s) <Standard-Names>"

5.3.3 Surveillance Audit

[A00VA02] applies

In addition, functioning of procedures for the periodic evaluation and review of compliance with relevant legislation and regulations shall be audited.

Some standard specific aspects should be taken into account as follows:

For BCMS

- Documents required for certification:
  - Documented statements of the BCMS policy and objectives;
  - Scope of the BCMS;
  - Procedure(s) of the BCMS;
  - Documented business impact analysis;
  - Risk assessment report;
  - Business continuity strategy;
  - Incident response structure;
  - Business continuity plans/ Incident management plans
  - BCM exercising records.
- Changes to the documented system;
- Areas subject to change;
- Selected elements of applicable BCMS Standard, e.g. the system maintenance elements which are preventive and corrective action
- Other selected areas as appropriate.

For ISMS

- Communications with external parties as required by the ISMS standard ISO 27001
- Other documents required for certification:
  - Documented statements of the ISMS policy and objectives;
  - Scope of the ISMS;
  - Procedures and controls in support of the ISMS;
  - Description of the risk assessment methodology;
  - Risk assessment report;
  - Risk treatment plan;
  - Documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls;

  - Records required by ISO 27001;
  - Statement of Applicability.
- Changes to the documented system;
- Areas subject to change;
- Selected elements of ISO 27001, e.g. the system maintenance elements which are preventive and corrective action and selected controls and controls objectives
- Other selected areas as appropriate.
- Information security issues related threats to assets, vulnerabilities and impacts on to the client organization and justify this programme.

In the case, any relevant modification of SoA is identified by audit team, this shall be recorded in [A50F207e] and certificate shall be re-issued referring to modified version of SoA.

For SMS

- Documents required for certification:
  - documented statements of the SMS policy and objectives;
  - SMS policies and objectives
  - Area of application/scope of the SMS
  - Service management plan
  - Documented service level agreements
  - Documented processes and procedures as required by ISO 20000-1
  - Records required by the Standard.
- Changes to the documented system;
- Areas subject to change;
- Selected elements of ISO 20000-1, e.g. the system maintenance elements which are preventive and corrective action
- Other selected areas as appropriate.

5.3.4 Recertification Audit

[A00VA02] applies

5.3.5 Extension audit

[A00VA02] applies

5.3.6 Short-notice audit

[A00VA02] applies

5.4 Zertifizierung von Unternehmen mit mehreren Standorten

5.4 Multi-site certification

[A00VA03] applies - supplemented by [A50VA03A1] for ISMS and SMS

Note: Multi-Site certification is allowed only for organisations operating just one management system. An integrated management system covering all applicable requirements of different management system standards is seen as one management system.

5.5 Aussetzung, Zurückziehen, Wiederherstellung, Erneuerung, Verweigerung, Kündigung und Einschränkung des Geltungsbereichs von Zertifikaten

5.5 Suspension, withdrawal, restoring, renewing, refusing, cancellation and limitation of the scope of certificates

[A00VA02] applies

5.6 Kalkulation kombinierter Verfahren InfMS und QMS

5.6 Calculation of combined procedures and QMS

[A00VA02] applies with some modifications

Combination is just accepted between BCMS, ISMS, SMS and QMS standards.

6 Anlagen

6 Appendices

6.1 Ablaufschema Zertifizierungsperiode (A00F284)

6.1 Flowsheet Certification period (A00F284e)

[A00VA02] gilt

[A00VA02] applies

7 Mitgeltende Unterlagen

7 Other relevant documents

[A00VA02] gilt

[A00VA02] applies