KPMG's Certification Compliance and Methodology

Regulatory Compliance

KPMG's Certification Bodies SCESm 0071, SCESp 0127, FLCES 006, DAkkS D-ZE-20924-01-00 are officially accredited by the Swiss government's Accreditation Services SAS and German Accreditation Body DAkkS based on the norm ISO/IEC 17021-1 and ISO/IEC 17065 (www.sas.ch) to perform formal certification audits in various management systems and products domains.

KPMG focuses on digitalization, information governance and process quality. These areas are faced with three basic challenges that threaten the clients' business success:

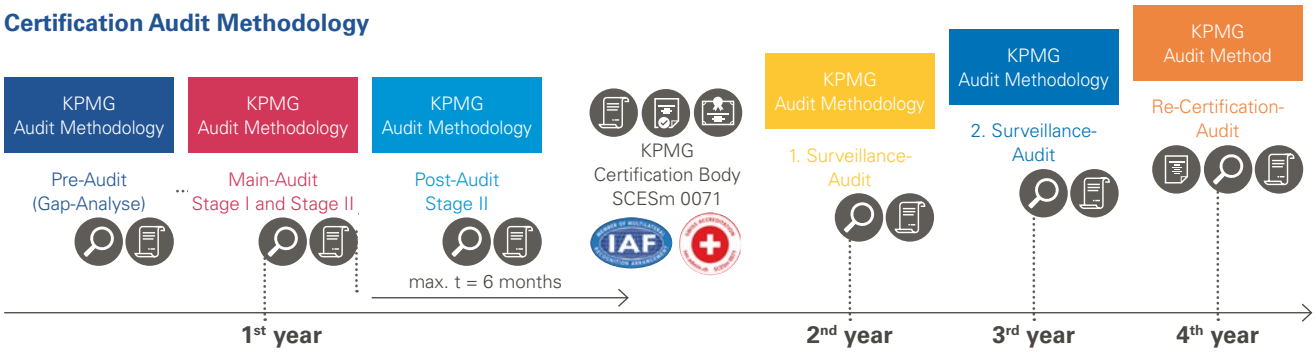
- Comply with customer requirements and government regulations and standards.
- Protect the organization through embedding quality and instituting best practices.
- Grow the organization, extending the customer reach and satisfaction, thereby increasing revenue.

Management systems allow organizations to meet these challenges by instilling best practices and validating, through certification, that they are properly established in the company.

Certification Audit

At the first audit, KPMG will examine whether or not the management systems fulfills the prerequisites for certification in accordance with the national regulation or international standard or norm. In particular, it will examine whether or not the organization has excluded components of its operation from the scope of processes, application, and IT-systems which necessarily form a part thereof.

Certification Audit Methodology



The KPMG Certification-Audit has, in principle, three phases:

- **Is-Situation status / Pre-Audit:** Overview and assessment on general selected controls.
- **Pre-Audit (Gap-Analyse):** in accordance with the selected regulation, standard or norm with interviews.
- **Stage I and II:** Main-Audit of the entire control framework (Documentation Review, Stage I) with interviews in accordance with the selected regulation, standard or norm including site inspection, technical implementation on configuration settings on IT-systems, all business processes and technical components of the effectively selected and pre-defined scope (Implementation Review, Stage II).
- **Post-Audit:** Verification audit to ensure that non-conformities and deviations have been improved and corrective actions measured.
- **Reporting:** KPMG will provide a detailed certification audit report (Stage I and Stage II) regarding the results of the control reviews carried out and the fulfillment of each the control objectives.
- **Certification Issuance:** KPMG will issue a certificate and confirmation letter based on the standard selected if all the control objectives have been successfully achieved.
- **Surveillance Audits:** The first and second surveillance audit comprises the review of pre-selected areas, such as: processes of the internal audit, management review, dedicated control objectives of regulation, the control objectives of preventive, detective and corrective measures and changes to the management system (process, legal, organizational, operational and IT/technical environment).

Further information about KPMG's Certification Methodology

Certification decision

The certification decision is taken by KPMG's certification body leader based on the information provided by the KPMG audit team (audit report, recommendation regarding the decision and additional remarks).

In order to maintain the certification surveillance audits and a follow-up audit for the renewal of the certificate will be performed at least annually by KPMG during the period of validity. To maintain the certification, corrective measures for identified non-conformities must be implemented within the set term by KPMG.

If the corrective measures are not carried out within the set term, the certificate will be withdrawn or the scope of the certification will be reduced. The client will be duly informed about any such measures KPMG intends to take.

For an expansion of the scope of the application of the certificate, the client must communicate this in writing to KPMG. KPMG will decide which audit procedure and which scope of audit is best suited to determine whether or not the change may be permitted. If the requirements for an expansion or limitation of the scope are shown to be fulfilled, a certificate will be issued for the new scope of application.

The validity of the certificate will be suspended if:

- The client does not carry out corrective measures for non-conformities identified in a surveillance audit, a re-assessment or an expansion audit within the agreed-upon time period.
- Changes at the client that may affect the capability of the management system are not communicated to KPMG.
- It is not made possible to carry out a surveillance audit, a re-assessment or an expansion assessment.
- It is detected that the certificate and the KPMG logo or trademark are misused.
- The client uses its certification in a manner which may discredit KPMG and makes declarations on its certification which KPMG deems misleading and unauthorized.

In the above-mentioned cases, KPMG will allow the client to implement corrective measures within the agreed upon term and to have the efficacy of the measures confirmed by a specific follow-up audit by KPMG in order to restore the certification. Otherwise, the certificate will be suspended for or limited to a term of a maximum of three months and subsequently, if appropriate, withdrawn or reduced in scope after a term of one month. In serious cases, the certification will be withdrawn with immediate effect. Except with respect to such withdrawal of certification, the client will be duly informed in writing regarding any imminent measures to be taken by the client.

Use and publication of certification and marks

KPMG will publish a complete list of the holders of a certificate at least once a year. This list will include the names of the certificate holders, the applicable standards, the scope of application and the locations to which the certificates relate.

The certificate issued by KPMG may only be published in full. The publication of excerpts of the certificate is not permitted without the prior written consent of KPMG.

The client has the obligation to ensure that third parties are not misled through statements in advertisements, other advertising material or any other means. The client shall further ensure that third parties are not confused regarding the object of the recognition as a certified company according to the respective certification standards pursuant to the certificate issued by KPMG.

The client has the right to display the certificate on all advertising material, product descriptions and packaging. The KPMG certification mark may be used on letters, etc., if KPMG has agreed to this use in writing. The KPMG certification mark may not be used on products.

The distribution to third parties of reports or correspondence delivered to the client by KPMG is permitted only with the written consent of KPMG. KPMG may link such permission to additional conditions.

Complaints and appeals

In cases of differences of opinion on the course of the certification process, the client may resort to the responsible member of the KPMG Executive Board who, with the reservation of the court of arbitration, has the ultimate power of decision.

Objections, complaints and disputes are to be submitted to KPMG. KPMG will keep records of the objections, complaints and disputes and will forward them to the responsible member of the KPMG Executive Board.

The responsible member of the KPMG Executive Board will examine carefully all objections, complaints and disputes. The person responsible will inform the audit team leader concerned and will determine further proceedings regarding the necessary investigation together with the audit team leader. If the objections, complaints and disputes are serious, the team leader will additionally inform the quality manager and the direct supervisor.

Process to ensure impartiality

KPMG has well established processes to ensure the impartiality of all certification activities.

The prospective engagement leader evaluates each prospective engagement in consultation with other senior personnel and KPMG Functional and/or National Quality & Risk Management as required. The evaluation identifies potential risks in relation to the engagement. A range of factors is considered as part of this evaluation including potential impartiality and conflict of interest issues.

Any potential impartiality or conflict of interest issues are documented and resolved prior to acceptance.

Depending on the overall risk assessment of the prospective client and engagement, additional safeguards may be introduced to help mitigate the identified risks.

KPMG will decline a prospective client or engagement if a potential impartiality or conflict issue cannot be resolved satisfactorily in accordance with professional and KPMG standards, or there are other quality and risk issues that cannot be appropriately mitigated.

KPMG provides certification services for the following certification schemes regarding the accreditation management system ISO/IEC 17021-1 and ISO/IEC 17065:

KPMG's accredited certification scheme

ISO/IEC 27001 Information Security Management System ISMS	ISO/IEC 27018 Cloud Security Management System Cloud MS	ISO/IEC 20000-1 IT Service Management System ITSM	BS 10008 Electronic Records Management System ERMS
ISO/IEC 22301 * Business Continuity Management (BCM) System	ISO 31000 * Risk Management	ISO/DIS 37001 Anti-bribery Management System	GeBüV and EIDI-V e-Invoicing Attestation Regulation Audit

DSG (SR 235.1), VDSG (SR 235.11), VDSZ (SR 235.13) Regulation incl. KVV Art.59a
Data Privacy and Data Protection Management System
DSMS

VEleS (SR 161.116), VEleS-TAV Art.9, Abs. 1, BSI-CC-PP-0037
Common Criteria Protection Profile Security Requirements
ISO 14298 (secure printing processes) and in accordance with CWA 15374

EPDG, EPDG-TOZ, EPDG-(IdP/CC)
Electronic Patient Records Management System (EPRMS)
Health care, University hospitals and regional hospitals, psychiatric clinics

ZertES (SR 943.03), VZertES (SR 943.032), TAV (SR 943.032.1)
ETSI EN 319 411-2 Qualified Electronic Signatures (QES)
ETSI EN 319 421, ETSI EN 319 422 Time Stamping Authorities (TSA)
WebTrust (ANSI X9.79)
CEN/TS 419.241 Sole Control 1 and 2 (Server Signing Signature Platform)
ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-1 till ETSI EN 319 412-5, ETSI TS 102.042
(NCP, NCP+, LCP, EVCP, EVCP+)
EN 419 211-2 till EN 419 211-6 (Signature Protection Profile)
EN 419 251-1 till EN 419 251-3 (Authentication Protection Profile)
EV / CapForum Extended Validation (EV) and SSL Signatures
IETF RFC 5280, IETF RFC 6960 OCSP, FIPS PUB 140-2 2001 Requirements for Trust Service Providers (TSP)
ISO/IEC 9594-8 (Directory / Attribute Certificate)
eIDAS Conformity Assessment Body (CAB), ISO/IEC 17065, EN 319.403

* For the time being, the norms and regulations marked with an asterisk (*) are not yet accredited by the Swiss Accreditation Services (Seco-SAS).

Why KPMG?

- KPMG's certification bodies SCESm 0071, SCESp 0127, FLCES 006, DAkkS D-ZE-20924-01-00 have a team of trained auditors and specialists with in-depth experience and credentials regarding the above mentioned standards, norms, regulations and risk management.
- KPMG has experience with attestation and certification in a wide variety of compliance regimes, certification schemes and important business and industry sector knowledge.
- KPMG is in a position to effectively help your organization to find the most efficient way of establishing a unified compliance program as well as a compliant controls environment with minimal redundancies.
- KPMG employs approved and tested certification methodologies that support your specific project goals and requirements.
- KPMG's clients benefit from a proven multidisciplinary approach with experts from various disciplines (e.g. information security, legal, compliance, risk management, process management etc).
- KPMG conformity assessment body (CAB) is in Switzerland and Europe the leading competence center for certification assessments according to the various standards/norms shown in the illustration on page 3.

Contacts

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch/consulting

Matthias Bossardt
Partner
Head of Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

Reto Grubenmann
Director
Head of Certification Services

+41 58 249 42 46
retogrubenmann@kpmg.com

KPMG's Certification Compliance and Methodology November 2018