IECQ OD 27001

Edition 1.0 2019-06

IECQ
OPERATIONAL DOCUMENT

IEC Quality Assessment System for Electronic Components (IECQ System)

Application of ISO/IEC 27001 for issuing IECQ ISMS approved process certification

IECQ OD 27001:2019-06(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IECQ OD 27001

Edition 1.0 2019-06

IECQ OPERATIONAL DOCUMENT

IEC Quality Assessment System for Electronic Components (IECQ System)

Application of ISO/IEC 27001 for issuing IECQ ISMS approved process certification

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

IECQ operational document OD 27001 –

Application of ISO/IEC 27001 for issuing IECQ ISMS approved process certification

FOREWORD

During the Busan 2018 IECQ Management Committee meeting, decisions 2018/07 and 2018/08 agreed to form an IECQ working group, WG 12, to explore further the possibility of integrating ISO/IEC 27000 series within the IECQ approved process (AP) scheme.

During the Singapore 2019 IECQ Management Committee meeting, WG 12 reported its study, including the business case study, into the integration of ISO/IEC 27001 to the IECQ AP scheme with IECQ MC agreeing to proceed with work on the new operational document (OD) and checklist.

This OD, prepared by WG 12 and approved by the IECQ Management Committee, sets out the process for:

1) qualification of IECQ certification bodies (CBs) that wish to include ISO/IEC 27000 series of standards within their IECQ AP scheme scope, and

2) procedures for processing applications and issuing certificates that include ISO/IEC 27000 series within the scope of certification

Document history

Date	Summary
2019-06-25	First edition approved by the IECQ Management Committee

Address:

IECQ Secretariat c/o IEC Sydney Office
The Executive Centre
Australia Square, Level 33
264 George Street
Sydney NSW 2000
Australia

Contact details:

Tel: +61 2 4628 4690
Fax:+61 2 4627 5285
info@iecq.org
www.iecq.org

INTRODUCTION

IECQ operational document OD 27001 details the application and use of the following international standard as part of the IECQ approved process (AP) scheme:

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

This OD covers the following:

- assessment and qualification of IECQ certification bodies (CBs) to issue IECQ certificates covering information security management systems (ISMS) to organizations that have been successfully assessed to ISO/IEC 27001, according to the IECQ AP scheme requirements
- requirements of IECQ CB staff to conduct assessments and audits to ISO/IEC 27001
- the method and system of assessment including allocated assessment days
- other information to ensure the consistent application of ISO/IEC 27001 by IECQ CBs

IECQ CBs conducting assessments to ISO/IEC 27001 shall record findings using the standard IECQ site assessment report (e.g. SAR 27001) as listed for use by IECQ CBs located on the IECQ website, under “Standard Forms”.

Further information concerning these procedures or any other aspect of the IECQ ISMS AP scheme or any other aspect of the IECQ System, may be obtained at www.iecq.org.

Application of ISO/IEC 27001 for issuing IECQ ISMS approved process certification

1 Overview and background

The need for organizations to maintain the security of information across many sectors continues to gain focus, including in the many industry sectors covered by the IECQ, for example the avionics sector and their related supply chain.

The generic IECQ approved process (AP) scheme provides for the independent assessment and issuing of an international IECQ certificate of conformity for organizations that have demonstrated compliance with declared standards and/or specifications, for example IEC 61340-5-1 for the management of electrostatic discharge (ESD).

With the growing need for organizations to provide independent proof of compliance with ISO/IEC 27001 for their information security management system (ISMS), industry has requested that IECQ certification bodies (CBs) be able to also cover the assessment and certification to ISO/IEC 27001 while conducting other IECQ assessments, e.g. ESD, avionics, HSPM and similar.

Therefore the IECQ Management Committee has integrated ISO/IEC 27001 into its IECQ AP scheme.

IECQ ISMS facility assessments under the IECQ AP scheme ensure a focus on the key technical and administrative elements that provide confidence that the requirements of ISO/IEC 27001 have been met.

2 IECQ CB acceptance for IECQ ISMS approved process certification

New CBs, not already participating in an IECQ scheme, are required to complete and submit form IECQ/MC/129G/Q to the IECQ secretariat and undergo the usual qualification and peer assessment required for all IECQ CBs according to IECQ 02. The IECQ peer assessment shall include assessment of the CBs compliance with the additional requirements of ISO/IEC 27006.

IECQ CBs, already participating in any of the IECQ schemes that seek to extend their scope to issue IECQ ISMS certification, shall apply to the IECQ secretariat using the IECQ CB scope extension application form IECQ/MC/130G/Q. IECQ CBs shall comply with any national regulations concerning their ability to offer IECQ ISMS certification and provide sufficient documentation to demonstrate the following:

- IECQ CB procedures include the implementation of the requirements for the IECQ AP scheme and requirements within this OD
- IECQ CB shall ensure that all aspects of the IECQ site assessment report SAR 27001 are integrated into their document system for all assessments to ISO/IEC 27001
- IECQ CB procedures include the technical review of assessments and the issuing of IECQ certificates of conformity

- IECQ CB shall have clearly recorded their IECQ lead auditors qualified for ISMS assessment work according to ISO/IEC 27001, including adequate evidence of training, qualifications, infield experience, etc., that address the requirements of ISO/IEC 17021-1 Annex A and the additional requirements for competence of personnel as specified in ISO/IEC 27006 (e.g. Clause 7.1 and its subclauses of ISO/IEC 27006:2015)
- IECQ CB shall ensure the use of qualified IECQ ISMS auditors for all IECQ ISMS assessments and how this is controlled
- IECQ CB statement of surveillance arrangements (SSA/NSSA) shall be updated to include the extension of scope to IECQ ISMS according to ISO/IEC 27001 under the IECQ AP scheme

The IECQ Secretary shall carry out or arrange to have conducted a review of the submitted documentation and provide a report with recommendation to the IECQ Executive. Such recommendations may include:

a) recommend that scope extension to the IECQ CB is granted
b) recommend to grant scope extension on the basis that the next IECQ peer assessment is conducted within X months/years
c) recommend that a site assessment of the IECQ CB be conducted prior to acceptance
d) recommend that scope extension not be granted and that the scope extension application is placed on hold or withdrawn

The IECQ Secretary shall provide a cost estimate for this review and the IECQ CB shall indicate its acceptance of this cost estimate prior to commencement of the review of submitted documentation.

Where the IECQ Executive grant the scope extension this shall be endorsed at the next CABC meeting.

3 IECQ CB auditors

IECQ approved process audits that include ISO/IEC 27001 shall be conducted by IECQ CB audit teams led by auditors which have been qualified by their IECQ CB as successfully completing the ISMS training and competence criteria set by the IECQ CB that aligns with Clause 2 above.

IECQ CBs shall select auditors in accordance with the requirements of ISO/IEC 27006.

4 IECQ ISMS approved certification

For a current list of IECQ CBs approved to conduct and issue IECQ certification that include ISO/IEC 27001, please visit the IECQ website: www.iecq.org.

5 The assessment and certification process

The general requirements for the assessment and certification of IECQ approved process, detailed in IECQ 03-2 apply concerning IECQ certification that include ISO/IEC 27001, along with the following additional requirements:

a) the IECQ CB audit and certification procedures are followed and shall align with the process requirements of Section 9 and its subclauses of ISO/IEC 27006

b) while the IECQ CB may utilize external resources for part of the process, e.g. use of contract auditors, the IECQ CB to whom application is made shall maintain control and be responsible for the overall certification process including the final certification decision and on-going certification maintenance

Companies and organizations seeking IECQ certification that covers ISMS are required to apply to an IECQ CB to arrange for the certification assessment/audit. The duration of the certification audit is based on the number of employees at a given location. In the planning of audit days, the IECQ CB shall ensure these are developed in accordance with ISO/IEC 27006.

A full certification audit is performed on a triennial basis providing no major non-conformities are raised during annual surveillance audits for each site that is to be covered by an IECQ approved process certificate that includes ISMS.

For the purposes of the IECQ approved process certification audit that includes ISO/IEC 27001, a “site” can include multiple buildings located in close proximity to each other that are:

- part of the same line of business
- have a common management and management system

As part of the IECQ approved process site assessment that includes ISO/IEC 27001, an assessment report shall be issued for the initial certification assessment and each surveillance assessment. The IECQ secretariat maintains standard site assessment report (e.g. SAR 27001) forms covering initial assessments, surveillance assessments and re-assessments.

6 Issue of international IECQ certificate based on previous certification

In situations where an international IECQ CB has previously issued ISO/IEC 27001 certification under its own scheme, it is possible to make use of the assessment and audits previously conducted in order to issue an IECQ certificate covering ISO/IEC 27001 by satisfying the requirements of Annex A. Where these requirements cannot be met then a site audit is required with the IECQ CB to determine the scope of the on-site audit to ensure that the requirements of this OD are met.

7 Certificate fees

IECQ certificate fees apply as follows: IECQ approved process company certificates, yearly (annual) fee CHF 100, paid to the IEC Central Office arranged by the IECQ CB. Multiple sites additional certificates and certificate surcharges shall apply in accordance with IECQ OD 011 Clause 4 and 5 respectively.

8 IECQ secretariat information

Further information concerning the IECQ ISMS certification or any of the other IECQ certification schemes may be obtained by contacting the IECQ secretariat as follows:

IECQ secretariat
info@iecq.org
www.iecq.org

Annex A
(normative)

Acceptance of previously issued ISO/IEC 27001 certification and audit data based on previously issued certification

A.1 Introduction

This annex sets out the conditions upon which IECQ certification can be issued based on ISO/IEC 27001 certification previously issued under another certification scheme.

A.2 Acceptable use

A.2.1 Where the IECQ CB has previously issued the ISO/IEC 27001 certification outside the IECQ System

IECQ CBs may use assessment and audit data obtained when issuing national ISO/IEC 27001 certification for the purposes of issuing IECQ certification to ISO/IEC 27001 only when ALL of the following criteria have been met:

a) the previous ISO/IEC 27001 certification has been issued by a CB accredited for that standard by an International Accreditation Forum (IAF) signatory to the relevant multi-lateral agreement (MLA)

b) the previous ISO/IEC 27001 certification is current and there are no outstanding non-conformances

c) the scope of the previous ISO/IEC 27001 certification and locations covered match those that are the subject of the IECQ certification

d) where under the previous ISO/IEC 27001 certification, it has been more than one year since the last surveillance audit, then the IECQ CB shall conduct a surveillance audit prior to the issue of IECQ certification

e) where under the previous ISO/IEC 27001 certification, it has been less than one year since the last surveillance audit, then the IECQ CB need not conduct a site visit audit prior to the issue of IECQ certification

f) the IECQ CB shall issue the IECQ certificate via the IECQ on-line certificate system and then commence surveillance audits that continue with the existing surveillance audit programme and utilize the IECQ SAR 27001 from the next surveillance audit onwards

A.2.2 Where a CB other than the IECQ CB has previously issued the ISO/IEC 27001 certification outside the IECQ System

IECQ CBs may use assessment and audit data obtained during the previous issuing of national ISO/IEC 27001 certification by other CBs providing:

a) items A.2.1 are met

b) the IECQ CB shall require the applicant organization to complete the checklist of ISO/IEC 27001, contained in IECQ SAR 27001 which, when completed, is to be submitted to the IECQ CB that shall review the completed checklist to satisfy itself that all requirements of ISO/IEC 27001 are met

c) the applicant organization shall provide the IECQ CB with a copy of the last CB audit report and the IECQ CB shall review this report to ensure that there are no outstanding major non-conformances

d) where a), b) and c) are satisfactorily completed, the IECQ CB may issue the IECQ certificate via the IECQ on-line certificate system and shall commence the on-going surveillance audits of the applicant organization

Where items a), b) and c) result in concerns raised by the IECQ CB, then the IECQ CB shall decide on any additional action which may include a site visit.

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch