KEURMERK

ZEKER-ONLINE

Zeker-OnLine is an independent, transparent Quality Mark for cloud services (also referred to as 'cloud solutions').

Section 6 Audit protocol

Version number 3.2
Commencement date: with immediate effect as from 1 February 2017
Working version 3.14

Contents

6. Audit protocol

6.1 Introduction

Online services providers seeking the *Keurmerk Zeker-OnLine* ('Secure Online Quality Mark') – the participants in the *Stichting Zeker-OnLine* – need to comply with stringent quality requirements that provide assurances for the reliable and continuous processing of transactions.
These quality requirements are specified in "Quality requirements and framework of standards".

For this reason an initial assurance engagement confirming compliance with these quality requirements is a condition attached to the award of the *Keurmerk Zeker-OnLine* Quality Mark. This assurance engagement must encompass a review of the design, implementation and operational effectiveness of the measures that the service provider has implemented to comply with the quality requirements.
Periodic audits or quick scans are required for the retention of the Quality Mark awarded after the initial audit. More information is enclosed below.

6.2 Audit cycle

To acquire and retain the *Keurmerk Zeker-OnLine*, audits are conducted in a three-year cycle. An initial audit of compliance with the framework of standards is required to obtain the Quality Mark. This audit concerns investigating the design, implementation and operational effectiveness, over a minimum period of six months, of the measures implemented by the service provider to comply with the audit objectives of Zeker-OnLine. Such an audit takes place within one year of participation being granted. The Board may grant an extension of this period on request.

After obtaining the *Keurmerk Zeker-OnLine* – subject to the initial audit on the basis of the full framework of standards – it is possible to opt for an audit on the basis of an abridged framework of standards in the following two years, after which a new period of three years begins. Each three-year period begins with a comprehensive audit on the basis of the full framework of standards, after which the choice is free for years two and three. The audit on the basis of an abridged framework of standards, also referred to as the Annual Update, is bound by conditions as described in Section 1.5. The audit periods are contiguous in the event that an audit period of 12 months is chosen. If an audit period shorter than 12 months is chosen, the period in each calendar year is the same as the previous period. Postponements may of course be submitted to the Board. The outcome of these audits and annual update – the assurance report – is delivered to the Executive Board within three months after the end of the audit period.

6.3 Appointment of an independent audit organisation/auditor

Participants may exercise their discretion in selecting the independent audit organisation that will conduct the audit provided that the following preconditions are met:

- the audit organisation possesses sufficient expertise to conduct the audit;
- the auditor affiliated with the audit organisation who will conduct the assurance engagement must be enrolled in the register of one of the following professional organisations:
  - The Netherlands Institute of Chartered Accountants (NBA) and/or
  - the *Nederlandse Organisatie van Register EDP-Auditors* ('The Netherlands Association of Registered EDP Auditors', NOREA);
- the audit team that will conduct the assurance engagement has relevant experience and expertise in the various fields of the framework of standards.

The participant shall issue the Foundation's Executive Board advance notification of the proposed audit organisation and/or auditor. The Foundation's Executive Board shall adopt a format for notifications of this nature.

The Foundation's Executive Board shall review whether the aforementioned conditions are met and shall issue a well-founded, binding recommendation on the selection of the audit organisation and auditor. On issuing this recommendation the Foundation's Executive Board accredits the audit organisation. When the Foundation's Executive Board rejects an audit organisation the participant may select a new audit organisation. The Foundation's Executive Board may also issue a recommendation naming a specific audit organisation.

The responsibility for the ultimate conclusion of the agreement commissioning the audit organisation/auditor to conduct the audit rests with the participant. Consequently, the agreement is concluded between the participant and the audit organisation/auditor and the participant shall settle the costs incurred in conducting the audit directly with the audit organisation/auditor.

6.4 Scope of the assignment

6.4.1 The auditor's assignment

The auditor receives the following assignment, in accordance with Article 8 of Standard 3402[1]:

a. obtain reasonable assurance about whether, in all material respects, based on suitable criteria:

1. the service organisation’s description of its system fairly presents the system that was designed and implemented throughout the specified period under review;
2. the internal controls related to the audit objectives stated in the framework of standards of Zeker-OnLine [and included] in the service organisation’s description of its system were suitably designed throughout the specified period under review;
3. the internal controls operated effectively to provide reasonable assurance that the audit objectives stated in the framework of standards of Zeker-OnLine and included in the description of the system by the service organisation were achieved throughout the specified period under review of at least six months.

b. Express an opinion in a written report about the matters stated in paragraph (a) above in accordance with the findings of the service organisation’s auditor.

A Zeker-OnLine reporting template has been established by the Foundation’s Executive Board, compliance with which is compulsory. This template is based on the reporting requirements under Standard 3402 (NBA) and the equivalent Guideline 3402 (NOREA). It is important that the confirmation of the instruction given by the Participant to the auditor specifies the use of the reporting template made compulsory by the Foundation.

The assignment shall be carried out in accordance with one of the following standards:

1. Standard 3402 of the NBA; or
2. Guideline 3402 of NOREA; or

[1] Accountancy Regulations Manual (Handleiding Regelgeving Accountancy, HRA) 2015 edition; Further Regulations on Auditing and Other Standards (Nadere voorschriften controle- en overige standaarden Standaard, NV COS); Standard 3402, Article 8.

3. ISAE 3402 of IFAC.

Wherever reference is made to Standard 3402, this reference means the three aforementioned standards. The developments concerning SOC 2 are being closely followed by the Foundation's Executive Board; as soon as this standard has a legal basis in the Netherlands, its applicability will be further specified.

The auditor's assignment must also state that the Participant releases the auditor from the obligation to maintain confidentiality as regards the Foundation's Executive Board, to the extent that is necessary to enable the Foundation's Executive Board to form an appropriate opinion; for example, during an explanatory meeting. Dossiers shall never be reviewed.

In sum, the confirmation of the assignment must include at least the scoping, reporting, use of template and release from confidentiality of information obligation as regards Zeker-OnLine for the purposes of the formation of opinion.

6.4.2 Auditor's procedures

The activities consist of establishing whether the provider of online services has taken measures such that the control objectives described in the framework of standards are being achieved. The measures which are taken by the provider of online services are derived from the control procedures described in the framework of standards.

The auditor determines the design and implementation as well as the operational effectiveness of the control procedures during a period of at least six months. The framework of standards has a 'principle-based' design, whereby control procedures are an important elaboration of the minimum required level with which the risks pertaining to the control objectives are mitigated. Deviations from the control procedures mentioned can be accepted by an auditor in the event of there being compensatory measures. If an exception to the control procedure is established and this procedure is replaced with a compensatory measure or measures, this measure is or these measures are incorporated into the reporting with a description of the nature of this compensatory control procedure. It is up to the auditor to assess whether this compensatory measure covers to a reasonable degree the risks for the aforementioned control objective. If the Foundation's Executive Board does not regard a measure as a complete replacement for the control procedure referred to in the framework of standards, the principles of 'due process' are applied (review with findings, hearing both sides, determining position). If the auditor is unable to agree to the Board's position, contact is made with the Participant. Both the participant and the Foundation's Executive Board may also decide to put this measure to the participants' council or the chair of the participants' council. As this process may delay the issuing of the certificate, the Board advises that significant changes are communicated in good time; for example, just after a 'zero measurement'. The participant may also independently submit a proposal for adjusting a control procedure to the standards committee, so this measure may possibly be included in a revised framework of standards.

The Foundation has opted for the application of Standard 3402, since this standard prescribes the correct set of activities. The administrative software will mainly be used for financial processes. A Standard 3402 report also ensures that accountants can make use of the activities carried out by the service organisation in the context of obtaining the *Keurmerk Zeker-OnLine* within the scope of an annual accounts audit. The activities can therefore serve several purposes. With the expansion to various other applications as portals, the choice for a standard will be jointly reviewed with the IT auditor.

6.4.3 Making use of subcontractors

The quality mark is granted to the service across the board. A software supplier may make use of subcontractors for housing services and hosting services, for example. The control procedures relating to the

subcontractors must be included in the audit of the Participant. If the control procedures of the subcontractor are incorporated with the aid of an underlying assurance report, it should be stated in the Standard 3402 type 2 report from the auditor what its weighting has been. If use is made of the Standard 3402 type 2 report from the subcontractor, this report must not be more than two months old when the Standard 3402 type 2 is submitted by the Participant. In this situation, it is recommended that the auditor consults with the Participant at an early stage as regards the period of the audit as well as the audit of the subcontractor/hosting service provider.

Example regarding period of validity of underlying report:

Audit of the Participant

Period of investigation: 1 April 2016 to 30 September 2016 inclusive

Submission of report: no later than 15 January 2017

Report from subcontractor

Period of investigation: 1 October 2015 to 30 September 2016 inclusive

Submission of report: 15 November 2016

The submission date of the report from the subcontractor determines the two-month period; in this example, the report from the Participant must not be submitted later that 15 January 2017: i.e. 15 November 2016 plus two months.

The basis of the two months lies in the term of validity of the report on the underlying period; its assurance decreases as this report ages.

Please note:

The IT auditor of the Participant must draw the overall conclusion as to whether the service is provided by the Participant in accordance with the framework of standards of Zeker-OnLine. This conclusion must be clearly indicated in the terms of reference and the report of the IT auditor.

6.4.4 Auditor's Assurance Report

The auditor publishes a report on their activities in the format made compulsory by the Foundation, as provided by the secretariat. This format is issued during the auditor's accreditation and is compulsory in order to be eligible for the *Keurmerk Zeker-OnLine*. The objectives and internal control procedures are hereby fully taken over from the most recent version of the framework of standards of Zeker-OnLine. A carve-out with regard to a subcontracted service by the IT auditor does not give any indemnity against complying with the objectives as formulated in the most recent version of the framework of standards. The report or supplementary report must show that the Participant is providing the service in accordance with the most recent version of the framework of standards.

6.5 Annual update

Zeker-OnLine provides for a full-scope audit during the application for the Quality Mark as well as an extension for the following years. Under certain conditions, in the event of an extension, use can be made of the audit on the basis of an abridged framework of standards (hereinafter: 'Annual Update'). The Annual Update is applicable on certain conditions. This option is not available to Quality Mark holders who have made substantial changes to the internal control, which cannot be assessed using this limited audit. The decision as to whether a change to the internal control qualifies as significant, and therefore necessitates a comprehensive audit, is reserved to the auditor. Consultation with the Participant on this matter is self-evident; consultation

with the Foundation's Executive Board is possible. Apart from this matter, there is an active obligation to disclose information in the event of significant changes to the administrative organisation and/or business operations, both to the IT auditor and to the board of Zeker-OnLine. Changes are significant if it cannot be unreservedly established that the service complies with the framework of standards of Zeker-OnLine. Examples may be changes in the ownership structure and a change of major subcontractors.

The Annual Update is based on the following assumptions:

1. The control framework consists to a large extent of control procedures of which, if they have been implemented, it is expected that these control procedures will continue to cover the control objectives for a period of three years. The Participant is asked to confirm these control procedures, which pertain to the structure of the control organisation, in years 2 and 3 by means of a description of the internal service organisation.
2. As a result of the above, the control procedures from the legal and application layer are in principle ineligible for the audit in years 2 and 3.
3. Current developments or specific changes from the Foundation's Executive Board should be incorporated into the description of the internal service organisation or added to the Annual Update carried out by the IT auditor depending on the nature of the measure.
4. Control procedures of which only the design and implementation has been determined on account of unavailability of test items during the audit period should explicitly be incorporated into the Annual Update of years 2 and 3.

Reporting in years 2 and 3 takes place on the basis of Standard 3402 and comprises:

1. the service organisation's description of its system, which fairly presents the system that was designed and implemented throughout the specified period under review;
2. the internal controls related to the audit objectives stated in the framework of standards of Zeker-OnLine and included in the service organisation's description of its system, and whether these controls were suitably designed throughout the specified period under review;
3. the internal controls audited, which were necessary to provide reasonable assurance that the internal control objectives stated in the description were achieved, operated effectively as designed throughout the specified period under review.

The IT Auditor is asked to report in accordance with Standard 3402 on the design, implementation and operational effectiveness of the control procedures over a period of six months. The measures selected for the Annual Update have been incorporated into the Annual Update template. This template is provided to the Quality Mark holders.

6.6 Further audit and withdrawal of Quality Mark

As indicated in Section 6.2, the audit cycle involves a period of three years, consisting of a comprehensive audit followed by two Annual Updates. If, in the interim, the Foundation's Executive Board has good reason to believe that a supplementary audit is required in order to determine whether the Quality Mark may be retained by a Service, the Participant shall arrange to have a new audit carried out and shall bear all the costs thereof.

If it appears in years 2 and 3 that the assurance offered by the *Keurmerk Zeker-OnLine* is coming under pressure, the Foundation's Executive Board shall be entitled to demand a full interim audit.

The Participant has, also on the basis of the conditions for participants, an active obligation to disclose information to the Foundation concerning changes to the organisation, processes and quality system which have an influence on the service.

The pace of developments in the field of online service provision may result in additional measures or reformulations being included in the guideline to the framework of standards.

The outcome of the Annual Update or the full-scope audit determines whether the Participant may continue to carry the Quality Mark for the service. If instructions from the Foundation's Executive Board are not followed, or are not followed adequately or on time, it may result in the Quality Mark being withdrawn.