STICHTING BETROUWBARE AFREKENSYSTEMEN

Office: SBA
Overgoo 15, 2266 JZ Leidschendam
Tel.: 070-3206730
Email: s.vanwezel@keurmerkafrekensystemen
www.keurmerkafrekensystemen.nl

SELF-ASSESSMENT 2.0 FOR THE KEURMERK BETROUWBAAR AFREKENSYSTEEM (RELIABLE POS SYSTEM QUALITY MARK)

Version 2.0 13 March 2017

CONTENTS

1. INTRODUCTION AND BOOKMARKER

1.1 Purpose

The purpose of the 'Self-assessment for the Reliable POS System Quality Mark' is to determine, based on the description of the measures included in the POS system, whether the POS system qualifies for the Keurmerk Betrouwbaar Afrekensysteem (Reliable POS System Quality Mark, hereinafter: 'the Quality Mark').

The Quality Mark promotes the building and installation of POS systems that register the data of transactions correctly and completely in a verifiable manner and store the data reliably. POS systems with the Quality Mark provide a correct, complete and always reliable understanding of the registered transactions and events.

The document 'Standard for a Reliable POS System' describes the standard for POS systems that qualify for the Quality Mark.

The documents:
'Standard for a Reliable POS System' and 'Self-assessment for the Reliable POS System Quality Mark' are issued by the foundation Stichting Betrouwbare Afrekensystemen (hereinafter referred to as: 'SBA').

1.2 Procedure and general information

The self-assessment must be carried out and provided with supporting documents, clearly referenced in the relevant part of the self-assessment. The board of the foundation SBA will decide, after obtaining advice from an external IT auditor, whether the Quality Mark will be granted.

In **Chapter 2** the scope, the parts of the POS system that are covered by the Quality Mark, is described.
In **Chapter 3** a description is given, based on **four control objectives**, of the standard the POS system must comply with.
Chapter 4 contains the **questions** that identify the business and the POS system and give a general picture of the quality of the organization.
Chapter 5 contains the **questions** that must be answered and provided with evidence to show that the POS system complies with the standard in order to achieve the control objectives. The questions have been grouped based on the main features of the process within the POS system. The manner in which you provide the evidence is up to you. **Appendix 1** contains **examples** of measures by means of which the standard can be complied with and also examples of evidence. Developments do not stand still. Other good or better measures may comply with the standard.

The definitions used in this document are explained in the document 'Standard for a Reliable POS System'.

2. SCOPE OF THE QUALITY MARK

The Quality Mark is aimed at the POS system that supports and registers the sale of goods and services to consumers in exchange for direct payment. It is aimed at the POS system that serves to reduce the risks that arise because the management of the stock, the sale, the registration of the amount payable and the settlement through direct payment are all in one hand.

The scope of the Quality Mark is described in more detail in the document 'Standard for a Reliable POS System'.

3. CONTROL OBJECTIVES

3.1 Register all the events

Control objective:
The POS system supports the registration of all events from the start of the sales process.

Explanation:
Special events, such as discounts, returns, tips, voids, aborted transactions, withdrawals, and training, will be marked and stored as such. It is consequently possible to determine whether the transactions actually performed have also been registered and settled correctly, completely and promptly.
The data are a source of information for steering the business. The registration has a preventative effect, as it supports the primary purpose of a POS system: the completeness of the recognition of the sales.

Standard:
- The POS system supports the registration of all relevant events (including metadata such as who, what, when and where). These are all the actions and activities that result in the input or output of data in the POS system.
- The POS system makes the registration possible from the start of the sales process.
- Corrections are processed without changing the data of the original transaction. Additional changes are registered with an audit trail to the original transaction.

3.2 Integrity of the registrations

Control objective:
The processing and registering of the data entered is verifiably correct, complete and timely.
The POS system contains measures for safeguarding this integrity and does not contain or support any functionality that break this integrity.
It is clear with regard to each change or deletion of a registration what this was, who is responsible for it and where (which cash register / location) and when this happened.
This applies both to changes processed by the POS system and to any access of the database from outside the system.

Standards:
- The software is protected against unauthorized changes.
- The registered events are correct and complete and protected against unauthorized changes.
- Changes in registered events will remain transparent.
- The audit trail of changes in software and registrations will remain accessible and available.
- Database breaches from outside the POS system will be detected and registered.

3.3 Storing the registrations

Control objective:
All transactions, events, permanent and semi-permanent data will be stored during the legal retention period. The authenticity, integrity and verifiability are demonstrably safeguarded. Any breach will be countered and identified.
The non-repudiation of the data safeguards the evidentiary value.
The data can be delivered promptly and properly.

Standards:
- The registered data will be stored during the legal retention period of 7 (seven) years.
- The registered data are demonstrably authentic, have retained their integrity, are verifiable, and are protected against unauthorized and undocumented changes.
- The registered data can be made available within a reasonable period of time.
- The POS system ensures that backups are made regularly.
- The set of measures for storing the data during the retention period and protecting the data against unauthorized changes is documented.

3.4 Adequate disclosure and reliability of the reports

Control objective:
In order for the entrepreneur to be able to manage the business and ensure adequate accountability, the reports must provide a reliable and transparent picture of the registrations in the POS system. This means that all events must be registered and stored correctly, completely and promptly (control objectives 1 to 3).
The reports must be generated correctly, completely and promptly, and the correct relationships between registrations must be made, so the structure of the report can be verified.
The POS system ensures that the reports are consistent with the data and provides insight into this consistency.
Completeness and correctness means that it must be possible to ensure that the reports are consistent with the data.

Standards:
- The reports are accurate, prompt and complete and show how the report is structured.
- The POS system supports regular cashing up/daily closing.
- The POS system supports exporting to common formats, preferably the XML Audit File Afrekensystemen. The dataset to be delivered meets the requirements for the XML Audit File.

4. SELF-ASSESSMENT - IDENTIFICATION AND QUALITY OF THE ORGANIZATION

This chapter contains questions about the identity of the applicant of the Quality Mark, the quality of the organization and general questions about the POS system.

4.1 Information about your organization

4.1.1	Name of organization	_____
4.1.2	Address of organization	_____
4.1.3	Postal code	_____
4.1.4	Business address	_____
4.1.5	Name of contact person	_____
4.1.6	Job title	_____
4.1.7	Telephone number	_____
4.1.8	Email address	_____
4.1.9	Name of technical contact person	_____
4.1.10	Job title	_____
4.1.11	Telephone number	_____
4.1.12	Email address	_____
4.1.13	Name of contact person in the administration department	_____
4.1.14	Job title	_____
4.1.15	Telephone number	_____
4.1.16	Email address	_____
4.1.17	Website	_____
4.1.18	Affiliated trade association	_____
4.1.19	Chamber of Commerce number	_____
4.1.20	Tax number of organization	_____

4.2 Quality of your organization

4.2.1 Describe the market position of your company

Specify:

- core activities,
- type of software and other products, also those for which you are not applying for the Quality Mark,
- target groups.

4.2.2 Describe the nature and size of your company in general terms

Specify:

- number of employees per main task such as development, sales, helpdesk, logistics, general,
- scope of operations,
- market share,
- partnerships.

4.2.3 Describe, in general terms, the measures in your company that safeguard the development and quality of your products

Specify:

- manner of documentation,
- version management,
- quality management,
- management of source code,
- change management,
- access security,
- backup and recovery.

4.2.4 Is the quality of your organization assessed by external supervisors? If so, which parts and quality aspects are assessed and by whom?

4.2.5 Where can the documents be accessed that substantiate the answers to the above questions?

4.3 Information about your POS system

4.3.1 For which product are you applying for the Quality Mark?

- name,
- version,
- date on which the product will be available on the market,
- other relevant features, such as a serial number or set of product numbers

4.3.2 Describe, in general terms, the architecture and configuration of the product

Consider the following:

- hardware, including input devices and peripheral equipment,
- operating system,
- nature of the software,
- database management,
- data communication.

4.3.3 For each relevant part of the POS system, specify whether it is managed by the user, the supplier or a third party

If the ownership and management of a relevant part of the POS system rest with a third party, how is it ensured that this part complies with the Standard for a Reliable POS System?

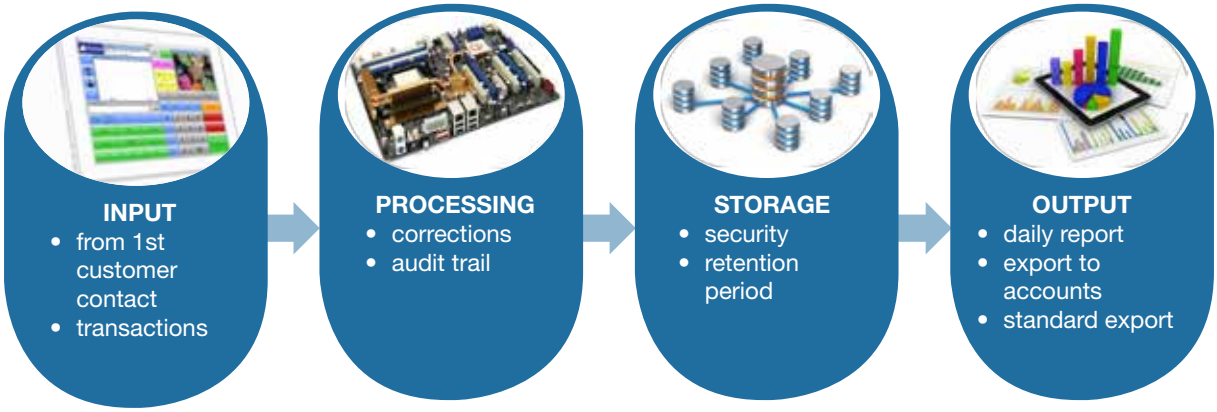
4.3.4 Describe the version management in general terms

Consider the following:

- When do relevant modifications and improvements result in an update, a new version or a new product?

5. SELF-ASSESSMENT – METHOD

The questions in the self-assessment have been grouped based on the order of the process within the POS system:



As regards the supporting evidence and implementation examples (also known as 'best practices') described in Appendix 1, we appeal to all participating parties to continue to provide these. This will help us learn from one another and continue to improve the quality of the Quality Mark.

5.1 Input

The POS system supports the user to ensure a correct, prompt, complete input of events, actions and transactions.

As regards the input of actions and transactions you must show:

5.1.1 **that it is registered who was responsible for the input of what and when;**

5.1.2 **how the completeness of the input is registered, for example by allocating sequencing and identification characteristics;**

5.1.3 **from which moment in the sales process an action or event that has been entered can no longer be changed and can therefore not be repudiated;**

5.1.4 **by means of which measures the non-repudiation is demonstrated;**

5.1.5 **that actions are registered such as:**
- **starting up, logging in, opening the cash drawer,**
- **changing parameters in training mode,**
- **connecting peripheral equipment such as input devices and receipt printers;**

5.1.6 **that the action, such as the input of the customer relationship, ordering, scanning, keying in the sales, paying, making corrections if necessary, right up to completing the transaction, is registered, even if the sales process is not completed;**

5.1.7 **how changes are entered and transparent after completion of the sales process;**

5.1.8 how the relationship with the original sales transaction is transparent;

5.1.9 that special events, such as discounts, returns, aborted transactions, withdrawals, own use, free distributions, opening the cash drawer, training and tips are identified in a specific manner;

5.1.10 which fields are filled in by the software;

5.1.11 which fields must in any case be filled in by the user;

5.1.12 which measures ensure that the correct sales price is charged;

5.1.13 in percentages (rounded off to 10%) to what degree the POS system complies with the Standard

_____%

5.2 Processing

The POS system processes the input of actions and transactions correctly, promptly and completely.

Show how the system:

5.2.1 ensures that all registrations are processed promptly and completely;

5.2.2 applies the correct calculation rules for each registration;

5.2.3 ensures that registrations of transactions are not deleted;

5.2.4 processes the input in the case of a calamity such as a power failure, computer malfunction or interrupted connection;

5.2.5 supports the user during the daily closing procedure;

5.2.6 shows the changes in functionalities made by the user;

5.2.7 in the case of a consolidation saves the primary data and thus maintains the audit trail.

5.2.8 Show in percentages (rounded off to 10%) to what degree the POS system complies with the Standard

_____%

5.3 Storage

There are various storage methods. From entirely in-house on local servers to fully outsourced to public cloud providers.
And somewhere in between: methods such as private cloud (shared infrastructure but own data management) and hybrid systems (a combination of physical servers and cloud servers from a data centre). As regards the Quality Mark the main distinguishing element is the extent to which the data storage is managed by the user or outsourced to the supplier or a third party.

Database managed by the user:
Filing: Show:

5.3.1 where and how the details from the POS system are filed during the legal retention period of 7 years;

5.3.2 to what extent the filing facility of the POS system forms part of the standard configuration.

Security: Show:

5.3.3 which measures ensure the correctness, completeness, timeliness, verifiability and thus evidentiary value of the registrations during the retention period;

5.3.4 the quality of the above measures, for example based on the results of penetration tests;

5.3.5 how an attempt to change data without authorization is detected, registered and reported. Who are these findings reported to?

5.3.6 which actions are carried out if the integrity of the database has been corrupted (for instance as a result of a direct change in the database made from outside the POS system);

5.3.7 which facilities the POS system offers for making a backup;

5.3.8 how the user is actively reminded to make a backup in good time and to carry out regular recovery tests. Is the user forced to make a backup? How?

5.3.9 to what extent the right to perform a recovery, which could affect the storage of data (such as data recovery, system recovery, hardware replacement) is reserved for expert and authorized personnel.

Database managed by the supplier or a third party: Show:

5.3.10 with which cloud provider(s) the data are stored;

5.3.11 where the servers are located (country and city/town);

5.3.12 whether the cloud provider has an ISAE 3402 certificate;

5.3.13 whether an SLA has been entered into with the cloud provider;

5.3.14 which measures have been taken to protect the data against risks concerning their integrity and confidentiality;

5.3.15 to what extent logging in is through a secure connection. How are the sessions protected against an attack by a malicious party ('Man-in-the-Browser')?

5.3.16 whether the data are available quickly and without restriction;

5.3.17 that the service is sufficiently available (outage percentage);

5.3.18 how the continuity of the service of the cloud provider is guaranteed;

5.3.19 to what extent all the actions are logged in the database and the log is accessible without restriction;

5.3.20 who the owner of the data is;

5.3.21 what agreements have been made about the actions to be taken on termination of the services;

5.3.22 in percentages (rounded off to 10%) to what degree the POS system complies with the Standard

_____%

5.4 Output

The output consists of reports, lists specifying the totals of the registrations and exports of selected data files.
Show:

5.4.1 5.4.1 which measures ensure that the output provides a correct, complete and timely picture of the registered data;

5.4.2 how users of reports can establish that the total of the registrations links up with the output;

5.4.3 how it is clear who structured the output and when;

5.4.4 how it is clear who created the output and when.

General: Show:

5.4.5 how it is clear on the basis of which variables the output of data was requested;

5.4.6 what the export possibilities are.
The best practice is exporting to the format XML Auditfile Afrekensysteem (XAA) (Audit File POS System);

5.4.7 which other export formats are possible;

5.4.8 **5.4.8 which measures ensure the correctness, completeness, timeliness, verifiability and thus evidentiary value of the output during the retention period;**

5.4.9 **in percentages (rounded off to 10%) to what degree the POS system complies with the Standard**

_____%

5.5 General

Show:

5.5.1 **5.5.1how the POS system supports the segregation of duties in the organization of the user;**

5.5.2 **which possibilities the POS system offers for showing at any given time which authorizations are being used;**

5.5.3 **how a user can see which authorizations that have been granted have changed;**

5.5.4 **which possibilities the POS system offers for showing at any given time which parameter settings it uses and has used in the past.**

Documentation: Show:

5.5.5 **how the functionalities of the POS system are documented;**

5.5.6 **where the documents are stored;**

5.5.7 **how you ensure that the documentation of the development of the POS system is kept up to date and matches the current version.**

Version management: Show:

5.5.8 **how you decide on the product name and version of the POS system;**

5.5.9 **how the history of the development of the POS system is registered;**

5.5.10 **how the POS system is able to convert data to a new version or a new POS system;**

5.5.11 **how the POS system is able to copy data from a previous version or a previous POS system;**

5.5.12 **how the software is protected against unauthorized changes;**

5.5.13 **which possibilities the POS system offers for showing at any given time which modules it uses and has used in the past;**

5.5.14 **in percentages (rounded off to 10%) to what degree the POS system complies with the Standard**

_____%

APPENDIX 1 Examples of evidence and implementation examples

Examples of evidence:

- Descriptions/manuals in combination with screen shots of the registrations with their features, including screen shots of a change where the audit trail has remained intact.
- Screen shots of checks on the completeness of processing (cross-checks; totals on daily reports, etc.).

Implementation examples:

5.1.2 Establish complete registrations through

- hash totals,
- cross-checks;
- totals on daily reports.

5.1.6 The fact that the sale, delivery and settlement are all in one hand means that it is es sential for controlling that process that all registrations continue to exist.

Shop:

The data registered after scanning or keying in the product will not be deleted. If the sale is cancelled before payment is made, the articles will not be removed but the transaction will be reversed, i.e. negative sale, so the original registrations are kept.

Catering establishment:

The data registered after the product is ordered will not be deleted.
If two beers are ordered and later changed to one beer and one water, one beer will be entered as a negative amount and one water will be entered, so the original registrations will be kept.

5.3.3 Correctness and completeness of the registrations can be ensured through hash totals with asymmetric encryption, with data characterizing the transactions and logging being included through an algorithm and a key in a separate table within the database

- By means of the table with hash codes it is determined whether the data in the transaction database have not been changed and
- by recalculating the hash codes and comparing them to the hash code table, it is determined whether the hash code table has retained its integrity and is still complete.

5.4.6 The possibility of exporting to the format XML Auditfile Afrekensysteem (XAA) (Audit File POS System) is highly recommended.