LNE' CERTIFICATION

CERTIFICATION STANDARDS FOR CASH REGISTER SYSTEMS

DOCUMENT REVISIONS

Version	Date	Reason for the update
1	29/11/2016	Initial version
1.1	07/12/2016	• Clarifications made to chapters I.3/ field of application (exclusion of electronic money) and V.4 / brand committee (deletion of the chairman and addition of the impossibility of veto right in accordance with standard NF X50-067) following the 1st brand committee of 06/12/2016.
1.2	12/12/2016	• Adjustment of the composition of the brand committee (V.4). • Adjustment of the appeals and complaints procedure (VI).
1.3	PROJECT	Whole document: Consideration of the DGFIP's FAQ on secure cash software dated 28/07/2017 § I.3: clarification of the scope of the standard §II.2: taking into account feedback for the drafting of conditions § III: clarification of the LNE Cash-desk System mark and the commitments of certification holders IV: clarification of the initial assessment and monitoring procedures. Glossary: added definitions
1.4	24/01/2019	• Taking into account the changes in the updated version of 04/07/2018 of the BOI-TVA-DECLA-30-10-30 Inclusion of clarifications from the July 28, 2017 FAQ Use of an open archive format Obligation to offer 3 levels of fencing Redefinition of the cash register system Details of the data concerned Requirement to trace purge/archive operations • Reorganization of the different parts of the repository • Clarification of the difference between certification and attestation • Details of the certification process • Redesign of quality requirements • Reorganization of technical requirements • Addition of the establishment identifier in the relevant data • Adding security for receipts • Updated examples of acceptable solutions in the mechanisms for ensuring data inalterability
1.5	PROJECT	• Correction of typos • Clarification of evaluation / audit vocabulary • Addition of major/minor NC classification criteria for the CMS • Adding certificate termination, suspension and withdrawal cases to the certificate tracking process • Alignment of activities related to the cash register system (chapter III) • Re-formatting of the data to be recorded listed in requirement n°3 and deletion of "Any data allowing the production of supporting documents (final or provisional)" from the list of data to be recorded • Clarification from the BOI added in the body of requirement 18 • Clarification of specific notes for requirements 3, 13, 21 • Clarification of audits of requirements 1, 2, 7, 8, 12, 15

BYCYB – 32 rue Guy Moquet – 92240 Malakoff , France – contact@bycyb.com
SAS au capital de 1 000 € – 942 788 845 R.C.S. Nanterre - TVA intra FR01942788845 - APE 7112B

Page 2 of 61

		• Content moved between the body of the requirement and the specific note: requirements 6, 7, 8 • Consistency of all references to the cash data defined in the various requirements of the standard • Removal of the notion of recipe/pre-prod environment and others in requirement n°5 on school mode

1.6	16/06/2021	• Replacement of the references to BOI-TVA-DECLA-30-10-30-20180704 by BOI-TVA-DECLA-30-10-30-20210519
		• Added footnote for "billing software" in the application section
		• Consideration of ISO 9001 certifications in the organizational audit period
		• Taking into account the changes of the updated version of 19/05/2021 of the BOI-TVA-DECLA-30-10-30
		    • Requirement 3: Add a statement that billing software is not required to record the POS identifier
		    • Requirement 6: Addition of an indication that the invoicing software is not required to complete the 3 closings subject to the provision of the total turnover for a specified period.
		    • Requirement 8: Clarification added to "Examples of Acceptable Solutions" section
		    • Requirement 11: Added clarification that records must be achievable over any period less than 7 years + added example of an acceptable solution
		    • Requirement 12: Addition of the concept of remote server in the examples of acceptable solutions
		    • Requirement 13: Added clarification that cumulative and summary data must never be purged
		    • Requirement 18 : Exclusion of the notion of traceability in the requirement and in the documentary and functional verifications
		    • Requirement 20: Clarification added in "Specific Notes" and "Examples of Acceptable Solutions
		    • Requirement 21: addition of an example of an acceptable solution
		    • Chapter III.2: deletion of the chapter on the publisher's commitments + renumbering of chapters
		    • Chapter 5 CMS: Renaming of chapter title to "Legal and Regulatory Watch
		    • Chapter 5 CMS: Deletion of the reference to receiving ESA newsletters
		    • Chapter 8 CMS: Removal of the commitment of subcontractors to comply with this standard
		    • Chapter 8 CMS: Reorganization of the chapter (last paragraph moved to first
		    • Added definition of billing software in the "lexicon" section
		• Clarification of requirement n°7 for the case of a cash register system used by several taxable persons
		    • Amendment to Requirement #3 regarding when transaction data must be recorded
		    • Amendment to Requirement #6 regarding staggered fiscal years
		    • Relaxation of Requirement #18 on terminal disconnection
		    • Integration of the new certification mark
		    • Page 66: deletion of the correspondence table
		    • Page layout

BYCYB – 32 rue Guy Moquet – 92240 Malakoff , France – contact@bycyb.com
SAS au capital de 1 000 € – 942 788 845 R.C.S. Nanterre - TVA intra FR01942788845 - APE 7112B

Page 3 of 61

1.7	30/05/2024	• Addition of certification modalities for products certified outside LNE.
		• Chapter III.2: addition of identification of responsibility relating to regulatory monitoring.
		• Chapter III.8: addition of checking the availability of the latest certified major version.
		• Chapter III.8: addition of verification of the publisher's communication with end customers of the availability of the latest certified major version in the case of non-automatic updating of systems at end customers
		• Chapter III.8: addition of an example of an acceptable solution with the possibility of using a licensing system to check the fleet of POS systems among end users.
		• Requirement 3: addition of the identification and inalterability of fields and their values when compliance with French regulations is configurable (documentary and functional).
		• Requirement 5: adding the identifier of the manager allowing the record of the transactions.
		• Requirement 8: addition of better formalization of key management.
		• Requirement 9: addition of management and identification of offline modes in the database.
		• Requirement 9: addition of an acceptable solution for identifying the use of offline mode as well as its maximum duration.
		• Requirement 9: addition of identification of supporting documents in electronic format.
		• Requirement 9: addition of checks carried out on the ticket.
		• Requirement 10: raised from note 36 in the body of the requirement.
		• Requirement 18: addition of identification and justification of a maximum time limit for the use of offline mode.
		• Requirement 18: addition of documentary verification of the recording of the maximum delay for offline mode.
		• Requirement 18: addition of checking the duration and causes of disconnections and offline mode.
		• Requirement 18: addition of verification of the identification of operations carried out in offline mode.
		• Requirement 19: addition of documentary verification of fields, their values and the integrity of settings so that the system complies with French regulations.
		• Requirement 19: addition of verification of integration and security of offline mode settings.
		• Requirement 19: Verify the number of licenses identified for end customers in the license use case.
		• Requirement 19: Verify that the French compliance parameters (fields and values) are attached to exports to the tax administration.
		• Modification of the operating methods of the brand committee.
		Context of 1.7 evolution:
		The update of the LNE ver 1.7 standard meets the following objectives:

BYCYB – 32 rue Guy Moquet – 92240 Malakoff , France – contact@bycyb.com
SAS au capital de 1 000 € – 942 788 845 R.C.S. Nanterre - TVA intra FR01942788845 - APE 7112B

Page 4 of 61

		- Improve robustness in the context of new types of fraud such as ghost cash register fraud.
		    Configuration of compliance with French regulations.
		    Offline Terms.
		- Specify the certification procedures for products certified outside the LNE
		- Various clarifications in particular concerning:
		    Communication to end customers during certificate withdrawal.
		    Traceability of the distribution of certified versions.
		    Key management.
		    Supporting documents in electronic format.
		    Information in the ticket
		- Editorial corrections.
		
		Transition terms for the repository in version 1.7:
		
		The standard version 1.7 comes into effect on the date of its publication. The repository in version 1.7 has a transition period, which ends on 09/30/2025. From September 30, 2024, all audits will be carried out according to version 1.7. Any deviation relating to these updated requirements must be subject to compliance noted before September 30, 2025 at the latest. All certificates must have been upgraded to version 1.7 by October 1st, 2025.
		On this date, all version 1.6 certificates will be withdrawn.
		
		Note: between now and September 30, 2024, the new requirements may be reviewed during the audit. Any discrepancy observed will be the subject of attention in the report. There will be no non-compliance with the new requirements during this period.

1.8	20/10/2025	**Updates in Version 1.8** • Incorporation of the update to **BOI-TVA-DECLA-30-10-30 dated 2025-04-16** and consideration of the **end of the self-attestation procedure**. • Inclusion of the **roles and responsibilities of LNE and BYCYB** within the certification process for cash register systems. • Clarification of the **wording of certain statements appearing on sales receipts**.

BYCYB – 32 rue Guy Moquet – 92240 Malakoff , France – contact@bycyb.com
SAS au capital de 1 000 € – 942 788 845 R.C.S. Nanterre - TVA intra FR01942788845 - APE 7112B

Page 5 of 61

TABLE OF CONTENTS

CHAPTER I: GENERAL

Introduction

Following the evolution of the **BOI**, a revision of Reference Framework **version 1.7** has been issued to ensure compliance.
Implementation Provisions for Version 1.8
- The **Reference Framework version 1.8** takes effect as of its publication date.
- Version 1.8 **does not introduce any new requirements** for systems that have already been certified.
- The impact applies **only to certificates updated to the higher version** within a period of **two (2) months** following the publication of the Reference Framework. Therefore, **no transition period** is defined.

I.1) Purpose & VAT taxable persons concerned

In order to combat VAT fraud linked to the use of systems that enable the concealment of revenue, the 2016 Finance Act introduced the obligation for all professionals subject to VAT, who make supplies of goods and services to private customers, recording the payments received in return by means of a cash register system, that this system be secure. This system must be certified by an independent body accredited by the COFRAC or certified by the publisher as being compliant with tax regulations, by means of an individual certificate[1].

Certification is a procedure whereby a third party, the certifying agency, provides a written insurance that an organizational system, process, person, product, or service complies with the requirements specified in a standard or reference system. It is governed by the Consumer Code.

This obligation affects all sectors of activity, it being recalled that the 2018 Finance Act excluded from the scheme taxable persons subject to VAT benefiting from the basic exemption scheme, those subject to the flat-rate agricultural VAT refund scheme, those carrying out exclusively VAT-exempt transactions[2] and those who carry out all of their transactions between professionals only (B to B).

This reference manual describes the terms and conditions for the certification of the cash register systems. It is mainly based on Article 88 of the French Finance Act No. 2015-1785 of 29 December 2015 and the official public finance bulletin BOI-TVA-DECLA-30-10-30-20250416, which defines the conditions of inalterability, security, conservation and archiving of transaction data that the system must meet. The standard aims to certify these 4

---

[1] BOI-TVA-DECLA-30-10-30-20250416: point 1.
[2] BOI-TVA-DECLA-30-10-30-20250416: point 25.

characteristics, the characterization of the system's tax scope and the system's versions, the documentation relating to the system, and the organization (CMS[3]) set up to ensure the production and delivery of the cash register systems that comply with the certified version.

I.2) Scope: definition of the cash register system

A payment system is a computer system (whatever its qualification: management, CRM, accounting, cashiering, invoicing[4], etc.) with a cashiering functionality.

A cashier's functionality consists in <u>memorizing **and** recording extra-accountably payments received in </u> return for a sale of goods or services, regardless of the means of payment. By extra-accounting, we mean that the payment recorded by the system **does not** <u>simultaneously</u>, <u>automatically</u>, <u>obligatorily </u> and <u>without human intervention, **generate** </u> an accounting entry in the accounting system[5].

Certain specific exclusions exist. Please refer to the BOI-TVA-DECLA-30-10-30-20250416. It is not the role of BYCYB to decide on the applicability of this BOI to the system concerned.

---

[3] CMS: Compliance Management System

[4] Invoicing software, i.e. a computer system allowing invoices to be issued between taxable persons for VAT purposes, containing the compulsory information provided for in Article 242 nonies A of Annex II to the CGI and complying with the conditions of Article 289 of the CGI, must be considered as cash management software or system as defined in I-B § 30, if it has a cash management function.

[5] BOI-TVA-DECLA-30-10-30-20250416: point 30.

CHAPTER II: CERTIFICATE ALLOCATION AND MONITORING PROCESS

II. 1) Ordering process

After an initial information gathering and discussion, BYCYB's sales department sends the initial questionnaire to the applicant for certification, which must be completed and returned to BYCYB in order to draw up the estimate. The sales department then sends the certification offer to the applicant. Once the order has been registered, the certification process can begin.

II. 2) Certification process

The certification process is divided into several successive stages. The main ones are :

1.   examination of the application file: documentary admissibility examination ;
2.   the completion of the initial assessment :

It is divided into 4 evaluation operations, each lasting at least one day:

▪   the <u>organisational audit</u> to ensure that the CMS in place complies with the requirements of Chapter III ;
▪   the <u>assessment of the documentary compliance of</u> the system with the requirements of Chapter IV ;
▪   the <u>assessment of the functional compliance of</u> the system with the requirements of Chapter IV ;
▪   the <u>assessment of the robustness of</u> the system to the requirements of Chapter IV ;

3.   feedback on non-conformance sheets where applicable;
4.   making certification decisions in a reading committee;
5.   the issue of the certificate once the certification decision has been ratified.

II. 2.1) Documentary admissibility review

Once the order has been registered, BYCYB sends the certification applicant the documentary admissibility form.

This form must be returned to BYCYB completed and accompanied by the technical file consisting of the documentation relating to the system. This documentation must be complete and provide a precise description of all the functions and mechanisms implemented to comply with the technical requirements of the LNE standard[6].

The documentary admissibility examination is not equivalent to the documentary evaluation carried out during the certification audit.

---

[6] CF: Chapter IV: Technical requirements for the certified cash register system (Requirement 1 and 2)

The examination of documentary admissibility consists of determining whether the assessment of the conformity of the cash register system is possible in view of the degree of completion of the technical file transmitted by the applicant. To do this, it is noted :

- if any of the documents requested in requirement 1 of Chapter IV are missing ;
- if all or part of the regulatory documentation is not in French;
- if the tax scope and version number management are well defined;
- whether the principle of the methods proposed to meet the requirements of Chapter IV is appropriate.

Once the documentary admissibility test has been completed, BYCYB informs the applicant of the result.

If this stage concludes that the application is inadmissible, it is up to the applicant for certification to reply to BYCYB by providing the missing documents. BYCYB's sales department will send a supplementary estimate if a second examination of documentary admissibility is required.

II. 2.2) Planning the initial assessment

If the documentary admissibility test is satisfactory, the file is admissible and BYCYB contacts the applicant to determine the dates and places of the various stages of the assessment.

The duration of the organizational audit can be increased if it is necessary to move on several sites, if subcontractors intervene in the design, the development, the tests, the integration, the manufacturing, the deployment/distribution, the configuration, the installation and/or the support of the system to be certified and are not followed by the certification holder, or if it is necessary to call upon an interpreter. It is fixed by default at one day. It can be reduced provided that the applicant of the certification has an ISO 9001 certified QMS for the activities covered by the standard (design, development, tests, integration, manufacturing, deployment/distribution, configuration, installation, support).

The duration of the documentary, functional and robustness assessments of a cash register system is related to its complexity; it is set by default at one day per assessment. It can be increased, especially after the documentary admissibility review, depending on the complexity of the cash register system (several human/machine interfaces, configurations and/or data flows to be tested, system architecture etc.).

II. 2.3) Conducting the initial assessment

Several appraisal operations can take place at the same time depending on the composition of the appraisal team.

It is recalled that the assessment operations are based on a sampling of the available information. The absence of non-conformity constitutes a presumption and not a proof of conformity with the requirements.

II.2.3.1): Organizational audit

The applicant for certification shall implement a Compliance Management System (CMS) to ensure that each cash register system, or upgrade, deployed meets the requirements of Chapter IV.

The requirements for this CMS are defined in Chapter III and their correct application is verified during the organisational audit.

The organisational audit of the CMS shall take place at the applicant's premises, preferably at the site where the design, development and testing activities for the system to be certified take place. When a holder wishes to certify several cash register systems, the organisational audit is pooled for all the systems if and only if the CMS documentation is common to all of them.
In case an applicant or certification holder has an ISO 9001 certification covering the activities and sites of design and development/production of cashiering systems, the duration of the organisational audit can be reduced.

The applicant for certification must ensure the availability of a contact person who is familiar with the implemented CMS, the company's organization and its processes, as well as any other person deemed relevant.

II.2.3.2) Robustness assessment

The objective of the robustness assessment of the cash register system is to verify compliance with the requirements defined in Chapter IV from a robustness point of view. The applicant for certification must ensure the availability of a :

- Technical expert mastering the design, development/manufacturing (knowing the source code), configuration and use of the payment system to be certified;
- A functional payment system in a test environment (in order to be able to easily modify the system date) with all the associated peripherals (printers, displays, remote control, etc.) connected and functional, and possible connections or configurations (to a PC, server or any other centralized system);
- Cash register system in a development environment (with full access to the source code, direct access to databases, servers etc.) ;
- access to user and technical documentation.

II.2.3.3) Literature review

The objective of the documentary assessment of the cash register system is to verify compliance with the requirements defined in chapter IV from a documentary point of view. The applicant for certification must ensure the availability of :

- a contact person who is familiar with the documentation and design of the cash register system to be certified;
- regulatory documentation[7] in French;

---

[7] CF: Chapter IV requirement 1

- additional documentation[8] in French or English;
- all the documentation for the assessor, as well as a relevant means of transfer. These documents will be kept by BYCYB as audit evidence.

II.2.3.4) Functional assessment

The functional assessment of the cash register system is intended to verify compliance with the requirements defined in Chapter IV from a functional point of view. The applicant for certification must ensure that :

- A contact person who is familiar with the design, development/manufacturing, configuration and operation of the POS system to be certified;
- A functional payment system in a test environment (in order to be able to easily modify the system date) with all the associated peripherals (printers, displays, remote control, etc.) connected and functional, and possible connections or configurations (to a PC, server or any other centralized system);
- A sufficiently large set of cash data to be able to carry out the repository's test cases: periodic closures (daily, monthly and annual), data synchronisation, archiving, etc.

It is reminded that the publisher is responsible for demonstrating the compliance of its product. Any lack of response or failure to provide evidence of compliance shall be recorded as a non-conformity.

II. 2.4) Response to non-conformity sheets

In case a non-conformity is noticed during one of the assessment operations, a form describing the NC[9] is written by the evaluator[10]/auditor[11]. This one is transmitted by the EM[12] to the applicant of the certification, at the time of the closing meeting of the evaluation.

There are two categories of NC:
1) NC 'system' of the CMS (Chapter III)

They can be minor or major.

A major NC is blocking for the certification: it must be corrected before the certification.

A minor NC is not blocking for the certification but will have to be corrected before the next follow-up audit, under penalty of certificate suspension.

Non-compliance is classified as **major** when, based on objective evidence:
- The non-compliance calls into question the compliance of the cash register system
    or
- There is a significant risk to the CMS ability to control the compliance of the cash register system
    or
- There is a systematic or repeated failure to meet a requirement (relating to the cash register system or the CMS)

---

[8] CF: Chapter IV requirement 2
[9] NC: Non-compliance
[10] Evaluator for stages 2/3/4: Evaluations of the Cashiering System (Chapter IV)
[11] Auditor for stage 1: organisational audit of the compliance management system (chapter III)
[12] EM: Evaluation Manager

2) <u>NC 'product' of the cash register system (chapter IV)</u>
Any product NC is blocking the certification: it must be corrected before the certification.
If the NC is only documentary, the EM or BYCYB may lift it after transmission of the appropriate documents.

The certification applicant then has a deadline fixed with the EM (from 3 to 5 weeks) to return each form completed with the analysis of the NC and the action taken.

After analysis of the actions proposed by the applicant for certification, the EM decides on its relevance and recommends the type of follow-up necessary for the NC.

II. 2.5) Opinion of the Evaluation Manager and review of the report
After receiving any NC sheets completed by the applicant for certification and the EM, BYCYB analyses the assessment report and the opinion of the assessment manager. After reading the report, it may request additional information from the applicant for certification, before it is submitted to the reading committee.

II. 2.6) Decision of the reading committee
The reading committee is responsible for giving an opinion on the certification decision in the process of awarding, monitoring, withdrawal or suspension of certificates. It is composed of at least :
- a representative of BYCYB management (who cannot intervene as certification project manager and who did not participate in the assessment);
- a certification project manager who is not in charge of the file;
- a certification project manager in charge of presenting the file.

The committee is chaired by the representative of BYCYB management and is responsible for :
- to examine the evaluation reports and to give an opinion and recommendation on the decisions to be taken, in particular on the type and duration of the follow-up of a NC;
- where appropriate, to examine, in the first instance, appeals against BYCYB decisions and to give an opinion on the action to be taken;
- assess the quality of the evaluation reports.

The certification decision is based on the examination of the elements of the file and the evaluation report. Each certification decision is materialised by the registration and, if necessary, the issue of a certificate.

Certificates are issued without a validity date and remain valid as long as no changes are made to the certified characteristics (fiscal scope). It is up to the company to notify BYCYB of any changes so that the necessary assessments can be carried out to revise the certificate.

II. 2.7) Certification procedures for products certified outside the LNE

Upon receipt of a certification request from a company already having certification according to a standard based on the requirements of BOI 30-10-30 and accredited according to standard 17065 by a recognized accreditation body, the terms of specific certification can be put in place.

The initial audit of companies already certified outside the LNE will be simplified by exempting them from the BYCYB review stage of documentary admissibility. However, the "certificate migration documentary verification" document must be completed by the company, in particular concerning the reference to the conformity documents in order to allow the evaluation to be carried out within the periods mentioned below.

The duration of the initial assessment for companies already certified outside LNE may be reduced;

For the rest of the terms of the initial audit, everything will be identical to the provisions already established in this framework.

II.3) Certificate monitoring

An annual surveillance assessment shall be carried out. The content of the annual assessment varies from case to case; its duration may not be less than one day.

In order to plan this surveillance, BYCYB sends a questionnaire to the company whose system has been certified to find out about changes since the previous assessment. Once the questionnaire has been returned, BYCYB draws up a monitoring offer based on the changes made.

The evaluation modalities according to the changes during the follow-up are as follows:
- **If the certified system has not been modified in any way :**
The annual follow-up assessment includes an audit of the registrant's CMS and checks to ensure that there are no changes to the system (footprint comparison). It lasts 1 day. The purpose of the assessment is to ensure that the CMS is maintained to produce cash systems identical to the certified one and that the traceability of the distributed systems is ensured.

- **If the certified system has undergone a change in its fiscal scope** (and therefore a major version change):
The annual follow-up assessment is considered by default as an initial assessment with a review of all the documentation, functional and robustness requirements listed in Chapter IV as well as the organizational requirements related to the CMS listed in Chapter III. Its duration depends on the changes made to the system.

Note: in the event of a change in the tax scope, the company must inform BYCYB of the changes made before it can distribute this version. The certificate only covers the system for a given major version.

- **If the certified system has undergone a minor modification** (i.e., no change in the tax scope):

The annual follow-up assessment includes an audit of the registrant's CMS and functional checks to ensure that subsequent minor releases of the cash register system continue to meet the 4 conditions of the cash data requirements defined in the BOI[13], and that there are no changes to the system's tax scope (footprint comparison). Its duration depends on the changes made to the system.

Once the order is placed, the steps below are identical to those for the initial evaluation:

1. follow-up evaluation planning ;
2. Conducting the follow-up evaluation (as per the previous evaluation modalities) ;
3. answers to possible NC sheets;
4. report review ;
5. decision of the reading committee.

II.4) Termination, suspension and withdrawal of the certificate

The grounds for termination, suspension or withdrawal of a certificate by the ESA are as follows:

- failure to comply with contractual requirements,
- refusal by the company to carry out the follow-up assessment within the time limit notified by BYCYB
- refusal by company to implement the required corrective action within the time limit notified by BYCYB
- the request for cancellation of all or part of the certification by the company.

BYCYB then formally notifies the holder of the suspension or withdrawal by registered letter with acknowledgement of receipt, indicating in the first case the conditions for lifting the suspension, in particular the corrective measures to be taken where appropriate.

In order to lift a suspension, BYCYB carries out the necessary checks to reinstate certification. If this is the case, the suspension is lifted and the certification is reinstated with notification to the holder.

When the certification is withdrawn or suspended, the former holder of the certification must cease all use of the mark under penalty of prosecution.

---

[13] BOI-TVA-DECLA-30-10-30-20250416: point 330.

Chapter III: Conformity Management System (CMS) Requirements

The applicant/certification holder shall implement, evaluate and maintain a Compliance Management System (CMS) to ensure that each cash register system or update placed on the market continuously meets the requirements of this standard.

This CMS must meet the requirements defined below.

Note: any future reference to recording information or producing a record refers to the requirements of III.13) of this chapter.

III.1) Background

The organization should identify and record the internal and external issues and risks (legal, reputational, financial, etc.) associated with the compliance of the cash register systems being marketed.

To do this, the organization must take into account the external regulatory and economic contexts, but also the internal context of the organization (resources, processes, suppliers, subcontractors, etc.). This can be done for example by implementing a risk management process, by establishing a risk map or a SWOT analysis.

III. 2) Roles and responsibilities

The company must be able to demonstrate that management has assigned and communicated responsibility and authority to the compliance function to:

a)   ensure that the conformity management system complies with this Chapter III ;

b)   analyse the technical requirements defined in Chapter IV ;

c)   decline them in functional specifications, which can be implemented ;

d)   Provide or organize training/information sessions for relevant employees to ensure that they are aware of the compliance requirements that apply to them;

e)   define compliance performance indicators ;

f)   monitor and measure these indicators ;

g)   Analyze the results to identify if corrective actions are needed;

h)   identify and manage compliance risks related to third parties such as suppliers, agents, distributors, consultants and subcontractors;

i)   Oversee the conditions of outsourcing to ensure that they take into account the compliance requirements defined in this standard.

j)   Ensure legal and regulatory monitoring.

Management shall ensure that the responsibilities and authorities for each activity related to the checkout system (design, development, testing, integration, manufacturing,

deployment/distribution, configuration, installation, support) are defined to ensure that the requirements defined in this standard are consistently implemented.

III. 3) Objectives and implementation of the CMS

The main objective of the CMS is to ensure that each cash register system or update put on the market meets the requirements of this standard at all times.

The company should identify and justify which activities may impact the compliance of the POS system (design, development, testing, integration, manufacturing, deployment/distribution, configuration, installation, support and evaluation of the effectiveness of the CMS).

For each activity that may have an impact on compliance, the company should define compliance objectives that should be :

- relevant ;
- consistent with the objectives of the CMS ;
- measurable ;
- communicated to the persons concerned;
- understood and applied ;
- monitored regularly by a compliance officer;
- updated as necessary;
- registered.

The organization must ensure that the CMS can achieve its intended outcomes and prevent or reduce risks. This includes ensuring that:
- the relevant actions to be implemented in correlation with
  o the issues ;
  o risks ;
  o requirements ;
- the integration of these actions within the activities concerned;
- the evaluation (and recording) of the effectiveness of these actions.

III. 4) Legal and regulatory monitoring

The organization must be able to identify new and changing legislation, directives, regulations, and compliance requirements to ensure the continued compliance of the POS system.

The organization may, for example:
- receive information bulletins from regulatory bodies (DGFIP, ministries, etc.);
- Follow or participate in professional working groups;
- subscribe to the appropriate newsletters;
- participate in professional events in the sector;
- regularly consult the websites of regulatory and certification bodies;
- seek legal advice;
- etc.

The impact of these changes should be assessed and the resulting actions (and changes to the CMS) should be carried out, monitored and recorded. If there are changes to the requirements, the functional specifications should clearly identify them.

III. 5) Establishment of compliance checks

For activities that may impact on the compliance of the cash register system (as defined in chapter III. 3), the organisation shall plan, implement and record effective controls for each cash register system activity to ensure that requirements are met and non-conformities are prevented or detected and corrected.

To do this, the company must:
- designate competent persons, who are familiar with the requirements of the standard, to carry out these checks;
- define the purpose of the control ;
- Define a suitable control frequency:
- record the results of these checks ;
- in case of non-conformity, record the analysis of the cause and the actions taken to correct the NC;
- ensure that the defined controls have been performed at the appropriate stages and that the results demonstrate the compliance of the cash register system with this standard.

These controls can be based on :
- documented, clear, practical and easy to follow policies, procedures, processes and operational work instructions;
- systems and fault reports ;
- code approvals or reviews;
- test plans and reports;
- a separation of incompatible roles and responsibilities ;
- automated processes ;
- annual compliance plans ;
- compliance audits.

III. 6) Design and development of the cash register system

The organization shall implement, in a controlled manner, and record a design process and an appropriate cash register system development or upgrade process to ensure the provision of cash register systems that meet the requirements of this standard.

The output of the design process that must be recorded is, at a minimum, the set of functional specifications related to compliance with this repository and the associated test plans.

The output of the development process is a prototype or update of a cash register system, compliant with this standard, and at least a record of the compliance test reports.

The following elements of the development process that must be defined and recorded (see IV. 1 Organizational and Maintenance File) must be applied as defined:

- the development method used (V cycle, W, agile method, organization's own method, etc.);
- source code management: explanation of the organization of directories, source code files, classes, packages, libraries, dll, etc. ;
- management of the version nomenclature (and in particular the management of major and minor version numbers)[14].

These processes must take into account:

- the conformity requirements of this standard ;
- the review of functional specifications and test reports by the function in charge of compliance.

The control of these processes must be based in particular on the achievement and recording of previously defined compliance objectives and controls and on the implementation, monitoring and recording of any action deemed necessary to remedy problems identified during controls.

In the event of a change to the design and/or development processes, the organization shall ensure, and record evidence, that the change does not adversely affect the compliance of the cash register system with this standard.

III. 7) Control of subcontractors

Outsourcing of certain activities (design, development, testing, integration, manufacturing, deployment/distribution, configuration, installation, support) related to the checkout system is possible provided that it, and the risks to the compliance of the checkout system, are controlled.

The organisation shall identify its critical suppliers/subcontractors, analyse the risks to the compliance of the cash register system related to subcontracting and implement any actions deemed necessary to reduce these risks. This information shall be recorded.

The conditions of subcontracting must be formalised and recorded (definition of the subcontractor, requirements, objectives and compliance checks, communication of results, procedure to be followed in the event of non-conformity).

The organisation shall monitor the conditions of outsourcing and the performance (and record it) of the outsourced activity by implementing controls to ensure that the compliance of the cash register system is maintained. It shall communicate these monitoring/evaluation procedures to the relevant outsourcer.

---

[14] CF: technical requirement n° 21

For example, it is possible to monitor these conditions via an audit of the subcontractor's quality management system by BYCYB or to take account of ISO 9001 certification by an accredited body for the above-mentioned activities related to the cash register systems and the sites concerned.

III. 8) Identification and traceability of distribution

Each distributed POS system must be uniquely identified (as well as the version distributed). This identification must allow:

- to ensure the traceability of the systems distributed on the market if applicable[15];
- to be able to make an update or a new installation if necessary (major vulnerability detected, patch related to compliance to be applied, etc.).
- to ensure that the latest certified major version is available for deployment to end customers.
- to ensure that the publisher has notified end customers of the availability of the latest certified major version in the event that end customers' systems are not automatically updated.

The organization shall maintain and continually update a record of the systems and versions distributed to its customers.

Example of an acceptable solution: It is possible to set up a licensing system to monitor the number of cash register systems deployed to each end customer.

III. 9) Communication with customers

The organization shall provide for the transmission to all customers where the certified cash register system is installed:

- all documents necessary for the proper functioning of the payment system (operating instructions, hardware requirements, etc.), whether these are provided by the publisher/manufacturer or a distributor;
- Support and training procedures where applicable;
- the responsibility commitments of clients with regard to the 2016 Finance Act (obligation to carry out closures, data retention, etc.) ;
- a description of the means of access to the cash data by the tax authorities as well as a user manual for the tax authorities describing the means of access to the cash data, a description of the format presented, and how to proceed with the data integrity check[16];
- the corresponding certificate.

In addition, it must ensure that the above documents are available to internal teams and users for 3 years after the end of distribution of each major version of the certified payment system.

The communication concerning the certification of the cash register system must not :

---

[15] A software in SAAS mode with a single instance is not affected.
[16] CF : technical requirement n° 19

- be ambiguous to the customer as to the name and version of the cash register system being certified;
- confuse the fact that the certification is for a cash register system and not for a company, a management system or a service.

The list of certified cash register systems is available on the BYCYB website, either via a search using the dedicated search engine or upon request from BYCYB, which provides information on the validity of a given certificate.

III. 10) Use of the LNE mark - Cash register system

The LNE is the owner of the "LNE numérique" certification mark.
The LNE has entrusted the management of the LNE certification related to cash register systems to BYCYB.
In its capacity as a certification body, BYCYB is responsible to the LNE for all activities entrusted to it, in accordance with the provisions of this Reference Framework.

Only companies that hold the "LNE cash register system" certification for one or more of their certified cash register systems may use the "LNE cash register system" mark on their products and communication media. The certification mark must be used in accordance with the current graphic charter published by BYCYB and reproduced on the current BYCYB website.

When the holder plans to affix the LNE mark (LNE mark - cash register system), he must comply with the provisions designed to ensure proper use of the mark:

- not to use the certification obtained in a way that could harm LNE, nor to make any statement or communication about the certification of its products that could be considered misleading or unauthorized;
- any reference to the certification before the notification of the certification is forbidden;
- in the event of withdrawal of certification, reference to the withdrawn certification is prohibited: any means of communication referring to it must cease to be used;
- make statements about the certification that are consistent with the certificate issued by BYCYB;
- reproduce the certificates in their entirety, with annexes if applicable, in the event of supply to a third party;
- Any reference to LNE cash register systems certification in advertising, in the presentation of any service, and on any commercial documents of any kind relating thereto must include at least the following information:
  - o the number of the certificate ;
  - o the address of the BYCYB website.

Any improper use of or reference to the "LNE cash register systems" mark, whether by the certificate holder or a third party, will be prosecuted in accordance with the regulations in force concerning misleading advertising and intellectual property.

III.11) Evaluation and improvement of the CMS performance

The organization shall implement the CMS monitoring, which consists of the collection and analysis of information to evaluate and improve the effectiveness of the CMS.

This monitoring includes the evaluation of the effectiveness :
- of the controls defined in III. 5, e.g. by analysis of the results of sample tests ;
- the treatment of previously identified non-conformities;
- actions taken to reduce the compliance risks of the cash register systems distributed;
- external service providers.

The organization shall take advantage of the CMS system monitoring to identify, implement and record any actions deemed appropriate to improve the CMS and reduce the risk of NC.

III.12) Anomaly handling

There can be no deviation from the requirements of this standard.

The organization shall ensure that non-conforming cashiering systems produced are identified and controlled to prevent their distribution and use.

If anomalies are detected during the checks defined in III.5, the organization must react (even after any distribution) as follows :
- analyze the anomaly: identify its causes in order to determine if it is necessary to take action to eliminate them so that the anomaly does not recur;
- implement actions to :
    - to correct the anomaly;
    - or to prevent the use of the cash register system(s) concerned, to warn its customers, and to recall the products or update them;
- evaluate the effectiveness of the actions implemented ;
- update the risks identified in III.1 if necessary;
- update the CMS if necessary.

The organization shall record information on the nature of the defect, its analysis, the actions taken and their results.

III.13) Records management

The organization shall control the records referred to in this standard and any others deemed relevant so that they are available, accessible and suitable for use, when and where they are needed. The organization shall ensure the storage, protection, retention and disposal of these records.

The records concerned are at least the following:
- risks (legal, reputational, financial, etc.) related to the compliance of the cash register systems (III. 1) ;
- compliance targets for each level and function for the activities concerned (III. 3) ;

- (III.3);
- relevant action following a change in the context and/or the CMS and the evaluation of its effectiveness (III. 4);
- compliance controls implemented and their results (III. 5 & III. 6) ;
- analysis of the cause of a NC and the actions taken as a result (III. 5 & III. 6) ;
- design process (III. 6) ;
- functional specifications related to compliance (III. 2 & III. 6) ;
- test plans (III. 6) ;
- development process & method (III. 6) ;
- test reports (III. 6) ;
- source code management (III. 6) ;
- definition of the fiscal perimeter (III. 6) ;
- management of the version nomenclature (III. 6) ;
- proof of no impact on compliance of a change in the design and development processes (III. 6) ;
- conditions of subcontracting (III. 7) ;
- results of outsourced processes (III. 7);
- identification of critical suppliers/subcontractors (III. 7) ;
- risk analysis of subcontracting compliance (III. 7) ;
- relevant action to reduce the risk associated with subcontracting (III. 7) ;
- registry of distributed systems and versions (III. 8) ;
- information on the NC, their analysis and actions taken (III.12).

When recording and updating recorded information, the organisation shall ensure that the following elements are defined and correct:
- identification and description: title, date, version number of the document ;
- format of the record (paper, electronic) ;
  - in the case of an electronic record: file name and extension (word, pdf, jpg, etc.);
- that the review/approval of the appropriateness and relevance of the information is carried out by the relevant persons prior to its release.

The organization shall ensure that externally generated documents are identified and prevent the use of outdated documents.

Chapter IV: Technical requirements for the certified cash register system

This chapter presents the technical requirements, which the certified cash register system must meet. The applicant for certification is free to demonstrate how it meets these requirements. Examples of acceptable solutions are given for some requirements.

The control methods are based on the evaluation of the documentation related to the cash register system, functional and robustness checks on the cash register system to be certified.

For each requirement, where applicable, the following are described: the title of the requirement, indications or examples of acceptable solution(s) and the documentary, functional and robustness verification methods.

IV.1) Documentation

The documentation of the payment system must describe all the functionalities and mechanisms implemented within the framework of the certification, allowing to meet all the technical requirements defined in this chapter. The organisation of this documentation must be described in a top-level document[17].

All of this documentation must be :
- kept on paper or in computerized form;
- retained until the end of the [third] year following the year in which the system ceased to be distributed[18];
- clearly and uniquely identified:
    - relevant title, in English or French;
    - document version number and/or document approval date.

Note: For each technical requirement, the expected documentation is listed in the "document verification" box.

The applicant of the certification is free to answer each of these requirements in the regulatory documentation or in the complementary documentation while respecting the constraints of these (languages of writing in particular).

---

[17] CF: IV.1) Requirement 2.
[18] CF: III.10) communication with clients

Requirement 1: Regulatory documentation [19]
The cash register system must be documented in terms of its design, operation, maintenance and use.
The documents listed below are covered by the tax authorities' right of communication, they must be written in French, separately and entitled as follows

     1. General design file,
     2. Functional specifications file,
     3. Technical architecture file,
     1. Organizational file,
     2. Maintenance file,
     3. Operating file,
     4. User file

---

[19] BOI-CF-COM-10-80-20160803: point 200.

Indications of what is expected :

These indications are not exhaustive, their only purpose is to have a better understanding of the expectations of each document.

General design file: Describes the system and its main operating principles as a whole, the equipment associated with the system to allow the collection of cash. Mapping of the different modules and their interactions. What OS and languages are used, network characteristics, brief description of any databases and how they are interfaced (conceptual & logical data models: MCD/MLD). Must also allow for unambiguous identification of the system: fiscal scope, minor/major versions.

Functional specifications file: Description of the identified use cases, points of attention and particular demands inherent to the system, defined during the design phase in order to validate that the solution will meet the expressly identified needs. In particular, the specifications linked to the requirements of the LNE reference system must be included.

Technical architecture file: describes in depth the technical implementation of the solution: technologies, algorithms (in particular signature and hashes used for data security), frameworks, protocols used; detailed architecture of the system (diagram with nature of the flows and the various components of the system). This file must cover all the processes carried out on the data to be secured, in particular their transport, backup, export, printing and display.

Organizational file: Describes the processes and organization in place for the design, development, configuration / deployment of the system? RACI, organization charts etc.

Maintenance file: intended to identify the follow-up of the evolutions/corrections of the product, the processes and the organization in place for the management of the vulnerabilities, the management of the licenses, the methods of updates of a version (corrective or evolutionary) and its delivery to the customer, the policy of versioning of the code mentioning the management of the major/minor versions within the meaning of the regulation

Description of the architecture of the source code (organization of the different code files, branches on the code manager) and identification of the portions concerned by the certification entering the tax scope.

Code version management policy (if applicable, the tool used: git, SVN, etc.) identifying the portions of code impacting the tax scope, linked to the functions of security, conservation, inalterability and archiving within the meaning of BOI TVA 30-10-30. This code, known as a "major version" or major/fiscal perimeter, cannot be modified without informing the LNE, in which case it will be subject to an additional assessment to verify its impact on compliance.

Operating file: Description of the possible configurations and settings of the system, its installation, hardware requirements, data backup methods, management of user rights, use and supervision of the system by the system administrator(s), as well as system replacement.

User file :

User's manual for the end user describing the system's functionalities, its operating instructions.

User manual for the tax administration describing precisely and simply the data access dedicated to the tax administration (with description of possible table fields, XML files, CSV files, etc.), in particular the methods of calculation of cumulative and summary data[20], the methods of verification of data integrity in the system [21]and of verification of archive integrity[22] as well as proof of completeness of data transfer to the centralizing system[23]. It may be included in the user manual or separate.

Documentary Audit :

Check that the regulatory documentation exists, is correctly identified (titles, version number and/or approval date) and is written in French.

Functional Audit :

Verify that a sample of documents for a system being released is available.

In the case of a certified system that has been out of use for less than 3 years, check that its documentation is available.

Robustness check :

Check that the technical documentation of the security methods is consistent with what is implemented.

Requirement 2: Additional documentation

The additional documentation is composed of all the documentation that allows the technical requirements of this standard to be met and that is not part of the regulatory documentation. It must be written in French or English.

The organisation shall provide an umbrella document describing the organisation of the documentation and summarising for each technical requirement which documents, paragraphs and page numbers are involved.

Documentary Audit :

Check that the supplementary documentation is correctly identified (titles, version number and approval date) and is written in French or English.

Functional Audit :

Verify that a sample of documents for a system being released is available.

In the case of a certified system that has been out of use for less than 3 years, check that its documentation is available.

Robustness check :

Check that the technical documentation of the security methods is consistent with what is implemented.

IV.2) Data recording

Requirement 3: Data to be recorded [24]

The cash register system must record all the cash data related to the completion of a transaction and its settlement. This data must be recorded as soon as a receipt (provisional, final or duplicate) can be issued. This data includes at least :

* Receipt number (transaction number if applicable),
* the POS[25] identifier (in the case of billing software, this data is not mandatory),
* a unique identifier of the establishment using the cash register system,
* the date and time of the transaction (year, month, day, hour, minute),
* the total amount including VAT of the transaction,

---

[20] See period totals and perpetual totals: CF requirement n°7

[21] CF requirement n°8

[22] CF requirement n°12

[23] CF requirement n°18

[24] BOI-TVA-DECLA-30-10-30-20250416: point 50-75-130

[25] POS: Point of Sale Terminal identified by a unique number (terminal number, cash register number, scale number, etc.). A terminal ensures the recording of the cash data locally, temporarily (pending the transfer of data to a centralized system) or in compliance with requirement no. 16 concerning the retention of data for a period of 6 years from the date of the last transaction recorded during the current fiscal year.

Requirement 3: Data to be recorded [24]

• the details of the items or services, i.e. for each line of the transaction :
     o wording,
     o quantity,
     o unit price,
     o total HT of the line,
     o associated VAT rate,
     o any other basic data[26] needed to calculate the total before tax of the line.
 • the payment method (and details of the amounts paid per payment method if payment is made via several payment methods),
 • the settlement date (if different from the transaction date),
 • any data enabling the traceability of the transaction and the integrity of the cash data to be guaranteed [27]

Specific note: **This data must be stored as such, as elementary data**, in the database and/or file system and not only be retrievable on the basis of a calculation, **such as the total excluding VAT of the line**.   The wording of the material or service must be recorded. A material code, material ID is not sufficient.   Any future reference to the "cash data" corresponds to the data required in this requirement plus the data generated by corrections (requirement n°4), the data required for requirement n°5 relating to school/test mode as well as the cumulative and summary data required for requirement n°7, the data required for the traceability of printing/reprinting of receipts defined in requirement n°9, the data required in requirement n°15 for the traceability of data purging, archiving and restoration operations, as well as the data required in requirement n°18 for the traceability of POS data transmission to the centralization system, if applicable.   In particular, data can be considered to be recorded when it is stored in the hard, non-volatile memory of the POS system (EEPROM type), i.e. it is not erased if the POS system is no longer supplied with power.
Examples of acceptable solutions: The unique identifier of the user establishment may be the establishment's SIRET number or the establishment's contact details (full address).
Documentary Audit :   Description of the method used to record all data in a comprehensive manner.   When parameters can affect compliance with French regulations, the parameters and their values should be explicitly identified in the documentation.
Functional Audit :   Perform a sample set of operations. Verify that all operations previously performed appear in the recorded data.   The following test cases are to be carried out if they are possible: application of discounts, application of promotions, application of loyalty advantages or equivalent, ticket reprints, etc.   When the parameters can affect compliance with French regulations, it is appropriate to verify that with the parameters and their values configured in accordance with the documentation, compliance with French regulations is effective, as well as verifying the impossibility of modifying these settings except after reset.

---

[26] Elementary data: data not obtained by calculation from other data
[27] CF requirement n°8

Requirement 4: Corrections [28]
If corrections (changes or reversals) are made to transactions by any means, these corrections are made by posting the corrective data through "plus" and "minus" transactions, not by directly changing the cash data posted.
Documentary Audit :
Verify from the full description of the transaction correction methods how the modified data is related to the original data and that the traceability of the modifications is ensured.
Functional Audit :
Test the operation of the system to ensure that corrections are made by "plus" and "minus" operations and not by direct changes to the original data recorded.
Verify by examining the database or file that the data is actually recorded, in case of correction.
Test cases must include the following: quantity modification, deletion of an article, deletion of a ticket, addition of an article to a ticket already finalized before payment, application of discounts, application of promotions, application of loyalty advantages or equivalent, etc.

Requirement 5: Test school mode [29]
Data generated, or simulated, through a "school" or "test" mode or function, allowing the recording of fictitious transactions, must be recorded and secured as the cash data but explicitly identified as being from this mode.
The identifier of the manager allowing the record of the transactions, as well as all the operations recorded during the use of this mode are part of the cash data. As such, these data must comply with all the requirements concerning them (recording, security, archiving).
Any voucher issued using this method must be identified as such by using the words "dummy", "simulation" or any other relevant wording in the background.
The use of the school mode must be visible from the display of the cashiering system.
If no such mode is present in the system this must be indicated in the documentation.

---

[28] BOI-TVA-DECLA-30-10-30-20250416: point 90 & 100.
[29] BOI-TVA-DECLA-30-10-30-20250416: point 90 & 150.

Examples of acceptable solutions: In order to identify the cash data generated by transaction simulations, it is possible, for example, to use a specific field in the database or a different database from the actual production data, provided that the same security mechanisms are used and that this data is properly integrated into the archive.
Documentary Audit :   Check from the full description of the mode concerned that :   the generated data is well recorded and secured like any cash data,   the responsible person's identifier and all operations carried out are well recorded and secured,   fictitious incoming payment data is clearly identified,   the supporting documents are clearly identified,   the system display identifies the mode appropriately.   Check that if no mode allows to simulate or generate data related to a fictitious transaction, this is explicit and argued if necessary in the documentation.
Functional Audit :   Enter the "school" or "test" mode or similar.   Verify in the database and on the supporting documents issued that the operation complies with the requirement and is consistent with the documentation.   Check that the data identifying the use of this school mode is secure by trying to modify it and by verifying the proper detection of the integrity error.

IV.3) Closings

Requirement 6: Annual, monthly and daily closings
The cash register system must provide daily, monthly and annual closing functionality. The annual closing should be based on the fiscal year when it does not coincide with the calendar year.   The cash register system must not allow new transactions to be recorded, or a transaction to be changed or reversed in a closed period. If closing is to be done by the user, the user must be informed of this possibility and of the responsibility that lies with him.   Invoicing software is not required to perform daily, monthly and annual closings, provided that it can provide, via a function, the total turnover recorded for a given period at the request of the administration.

Specific note:
These closings can be done automatically by the cash register system or by the user.
In the case of user closure, it remains the responsibility of the user of the cash register system to perform periodic closures.
Examples of acceptable solutions:
The user can be warned of the need to fence by any appropriate means (display on the system interface, user manual, contract, etc.).
Documentary Audit :
Check from the description of the closing functionality
if the 3 closing functions (daily, monthly and annual) are present,
that the functionality meets the requirements,
that if the functionality is not automatic, the user is warned of the obligation to perform the fences.
In the case of invoicing software, check if there is a daily, monthly and annual closing functionality or a functionality to provide on demand the total turnover recorded for a given period.
Functional Audit :
Record transactions and perform closings (at least 1 closing at each level) and verify the correct generation of closings.
Also check that it is not possible to post a new transaction or change/cancel a transaction in the closed period.
In the case of an invoicing software that does not perform daily, monthly and annual closing, check that the software is able to provide, via an on-demand functionality, the total turnover recorded for a given period.

Requirement 7: Cumulative and summary data [30]
For each closing, the cash register system must record and secure[31] the period-to-date total and the perpetual total like any other cash data. If the cash register system is changed, all counters are reset to zero. The counters of the old system must then be archived[32]. In the case of a system update, all counters must continue to be incremented without being reset to 0. In the case of a cash register system used by several taxable persons, the cumulative and summary data must be generated separately for each taxable person.
Specific note: The cumulative total of the period is the total of the sales settled since the opening of the period in question. It is a counter that is initialized to 0 at the opening of the period (daily, monthly or yearly) and whose value is stored at the closing. The perpetual total is the cumulative sales figures that have been counted since the start of the cash register system. It is a counter that never resets to 0 and whose value is stored periodically at each closing.
Documentary Audit : Verify from the documentation on cumulative and summary data that the method of calculating these totals is based on turnover, is precisely described and that these data are recorded for each closing (daily, monthly and annual).
Functional Audit : Verify on the basis of a sample of representative test data that the cash register system correctly calculates and records the period-to-date and perpetual totals for each of the closing periods.
Robustness check : Verify that the integrity and authenticity of cumulative and summary data is based on a robust mechanism.

---

[30] BOI-TVA-DECLA-30-10-30-20250416: point 170.
[31] CF requirement n°8
[32] CF requirement n°10

___

IV.4) Data security and inalterability

Requirement 8: Non-alterability of data [33]
The cash register system shall provide a mechanism to ensure and demonstrate that all cash data defined in the previous[34] requirements has not been altered since it was first recorded. This mechanism must be able to detect and demonstrate any modification or deletion of the cash data. The methods for managing keys and/or certificates must be documented, including at least the following aspects: the method of generating keys and/or certificates, the validity periods, the scope (whether a key/certificate per fund or shared between several funds), the renewal terms and the revocation mechanisms.

___

[33] BOI-TVA-DECLA-30-10-30-20250416: point 80 & 100.

[34] The data defined in requirement n°3, the corrective data defined in requirement n°4, the test-school mode data defined in requirement n°5, the cumulative and summary data defined in requirement n°7, the traceability data for printing/reprinting of receipts defined in requirement n°9, the data defined in requirement n°15 for the traceability of data purging, archiving and restoration operations, the data defined in requirement n°18 for the traceability of POS data transmission to the centralization system, if applicable.

Requirement 8: Non-alterability of data [33]

Examples of acceptable solutions:

The inalterability of the data can be guaranteed by :

1) the proof of authenticity and integrity of the data, which can be a chain of key fingerprints, or a chain of signatures of each record.

Authentication and integrity can be guaranteed by a signature mechanism (such as RSA-SSA-PSS, ECDSA) or a key fingerprint mechanism (HMAC). The key must be generated by a reliable process and the end user (the regulated professional) must not be able to know it or be easily guessed. The signature (or keyed fingerprint) of a transaction must include elements authenticating the previous transaction as well as the last recorded transaction (via a counter or other unique element) to ensure that no transaction has been deleted.

Regarding the choice of algorithms used, it is advisable to refer to the ANSSI's General Security Reference Guide. Beyond the choice of the algorithm, its implementation is equally important (management of keys for signature, key size, padding management, etc.).).

The following examples of key fingerprinting mechanisms are acceptable: HMAC-SHA-256, HMAC-SHA3.

The following examples of hash functions are not acceptable: SHA-1, MD5, CRC16, CRC32, and all other forms of non-cryptographic checksums including a CRC32 of an SHA256 fingerprint.

The following examples of data signature algorithms are acceptable: RSA-SSA-PSS, ECDSA. For the RSA algorithm, a minimum 1024-bit key is required. It is recommended to use a key of 2048 bits or more. For elliptic curves, their order must be at least 256 bits. The following examples of elliptic curves are acceptable: ed25519, Brainpool, P-256, ed448.

2) The signature or the taking of a key fingerprint of the whole stored data. In this case, for each transaction, the new signature or key fingerprint must be calculated on the entire data set after checking it against the old value.

3) Full control of write access to the data may be acceptable. The regulated professional must never be able to obtain write access to the data. It is possible that the system relies on an encrypted and signed database (for example, with the "encryption at rest" mechanism under Mongodb) for which the cryptographic key is not easily accessible by the user (use of key burying principles for example, or an external USB dongle with a license protection type mechanism)

Regardless of the solution chosen, in the case of a cash register system deployed on a workstation for which the user has administrator rights, it is necessary to prevent the data from being restored to a previous state. The operation must be detected or made impossible. It is possible to record, without the access of the user of the cash register system, the proof of integrity (signature, fingerprint) of the last record (in the case of a data chaining) or of the whole database if the system allows it.

These solutions are not exhaustive and can be used in conjunction with other solutions.

Certification standards for cashiering systems v1.8
Chapter IV: Technical requirements for the certified cash register system

---

Requirement 8: Non-alterability of data [33]
Documentary Audit :
Verify that the mechanisms ensuring the inalterability of the data are precisely described, including the cryptographic algorithms used. Verify that the data concerned by these mechanisms includes all the cash data to be secured :
all cash data defined in requirement 3,
all corrective data defined in requirement 4,
all test school mode data defined in requirement 5
cumulative and summary data as defined in requirement 7
The print/reprint traceability data defined in requirement 9
The traceability data of the data purging, archiving and restoration operations defined in requirement n°15.
the data defined in requirement n°18 for the traceability of the POS data transmission to the centralizing system, if applicable.
Functional Audit :
Verify the presence of a means of controlling the integrity of the data and its effectiveness by modifying it directly on disk or in the cash register system data base.

BYCYB
build your cyber

Page 37 of 61

Requirement 8: Non-alterability of data [33]

Robustness check :

Carry out a set of payment operations.

Log on to the device with all authorized means of access, and try to modify the operation data already recorded.

Verify, including through code auditing, that the recorded cash data is protected against alteration (modification, insertion, deletion or replacement) by :

   o   case 1): Verify that the secret (the key) is randomly generated and not accessible by an attacker.

Verify that each record is cryptographically linked to the record that precedes it chronologically, by including in the calculation of the cryptographic fingerprint of the current record elements authenticating the previous record, as well as the date and time.

Verify that the signature or key fingerprint algorithm is compliant. Verify on the device, and by sampling, the consistency of a chain for a set of records containing corrections (modifications and cancellations).

Check the security of the elements at the end of the chain, especially against their removal.

   o   case 2): Verify that the secret (the key) is randomly generated and not accessible by an attacker. Verify that at each record, the previous signature of the data set is verified before it is overwritten.

   o   case 3):

Check that the means of protection providing the same level of security as the previous examples are implemented. In the case of a control based on a trusted third party, verify the provisions and SLAs taken concerning these means of protection from the contracts, terms and conditions, descriptions of the management of rights and access control, RACI of the teams intervening on the data, proof of traceability of maintenance operations as well as any other document deemed relevant.

Carry out a robustness analysis on the mechanism ensuring the security of records (examples of tests to be carried out: validation of the chain of electronic certificates, correct use and implementation of the cryptographic mechanisms used and compliance with the state of the art, etc.).

Check that the security of data flows is based on secure channels (e.g. HTTPS/TLS).

Verify that restoring a database or folder containing the protected data is prevented or detected.

Verify that all cash data affected by requirements 3, 4, 5, 7 and 15 are covered by the security mechanisms.

Conclude on the ability of the system to ensure data integrity and authenticity.

Requirement 9: Securing of supporting documents

The cash register system must be able to distinguish and unambiguously identify receipts issued before payment from receipts issued after payment.

Any reprinted receipt must be marked "duplicata".

The system must ensure the traceability of printouts and reprints of receipts (final or provisional) in a secure manner. but also sending supporting documents in electronic format.

The information on the receipts must be consistent with the cash data recorded by the cash register system.

Receipts shall indicate that the cash register system is certified by LNE.

For centralizing systems, in the case where the system is in offline mode, this state must appear on the exports.

The procedure for issuing supporting documents in electronic format must be clearly documented, including sending protocols and methods for managing originals and duplicates.

It is recommended that any failure to print or send proof in digital format is recorded securely.

Specific note:
Invoice, note, receipt, ticket, tickets are all receipts.
These supporting documents can be in paper form or in electronic form (pdf, etc.).
It is recommended that the transaction signature be included on the ticket in order to demonstrate the ability to establish a definite and tamper-proof link between each ticket and the corresponding transaction recorded in the database.
Examples of acceptable solutions:
It is possible to indicate "valid for payment", "provisional", "pro-forma", "unpaid" on the receipt before payment and to indicate "payment made", "payment received", on the receipt of payment.
In cases where the same bill is shared among several customers, it is possible to issue a first receipt identified as provisional, and then issue receipts after payment, the sum of the totals of which correspond to the total of the provisional receipt.
It is possible to ensure the traceability of receipt prints/reprints by recording and securing the number of prints of each receipt or to trace each print/reprint by recording the date, time and receipt number (or transaction number if applicable) in a secure log/event log with the same level of security as defined in requirement #8.
It is possible to add a field to the database to identify operations carried out in offline mode.
It is possible to mention on the ticket the type of mode used to generate the ticket.
It is possible to mention the digital signature of the operation on the ticket.
It is possible to track the use of offline mode as well as its maximum duration.
It is possible to add the LNE certificate number to the ticket and/or invoice.
It is possible not to indicate the VAT rate on receipts as long as no payment has been collected or the final receipt has not been issued.
In order to ensure the traceability and transparency of the receipts issued, each receipt must indicate that the payment system is certified. The wording "Système de Caisse Certifié LNE" is recommended. However, the wording "Système certifié LNE" is acceptable, provided that it does not create any ambiguity as to the scope of the certification.
Documentary audit
Verify from the description of the methods of printing the credentials that all requirements are anticipated and documented.
Verify that the procedure for issuing electronic receipts is clearly documented, including sending protocols and procedures for managing originals and duplicates.
Functional verification
Check that the supporting documents issued before and after payment are clearly identifiable without any ambiguity.
Check according to the different use cases of the system, the consistency of the issued receipts with the recorded transactions as well as the update of the basic print counters.
Check in the case of a split bill/note that the sum of the amounts of the different receipts is equal to the amount including tax of the initial transaction.
Check the traceability of the physical and electronic supporting documents generated.
Check that operations carried out in offline mode are clearly identified on the ticket and in the system.
Check the presence of the SIRET.
Check the presence of the mention "Systeme de Caisse Certifié LNE ".

IV.5) Archiving of the cash data

Requirement 10: Data archiving
The cash register system must provide an archiving function for users, allowing the export of The data defined in requirement n°3, the corrective data defined in requirement n°4, the test-school mode data defined in requirement n°5, the cumulative and summary data defined in requirement n°7, the traceability data for printing/reprinting of receipts defined in requirement n°9, the data defined in requirement n°15 for the traceability of data purging, archiving and restoration operations, the data defined in requirement n°18 for the traceability of POS data transmission to the centralization system, if applicable·fixed and time-stamped cash data in an open[35] format.   If the cash register system is changed, the cumulative and summary data[36] must be archived.
Specific note   The archiving functionality should not be confused with a long-term data backup solution. This involves exporting transaction data from the system in an open and secure format, with a timestamp and security measures in place to seal data, in order to protect against data loss due to hardware problems, security breaches, changes to the payment system, or any other reason. It is a way for the taxpayer to be able to keep his cash data independently of the cash register system and to be able to communicate them to the tax authorities in case of an audit.   It is not the responsibility of the cash register system's publisher to carry out the archiving. However, the system must allow its user to archive the data. It is the responsibility of the system user to carry out the archiving.
Example of acceptable solutions: The following formats for archive data are acceptable open formats: ods, xlsx, odb, csv, json, xml, txt. If the archive data is compressed, the following compression formats are acceptable open formats: zip, 7z, gz, bz2, tar, rar.   On the other hand, the following formats are closed or proprietary formats that are not acceptable: xls, mdb.
Documentary audit   Check from the description of the archiving functionality that it exists, that a user of the payment system can use it and is aware of it, that the format is open and that the data in the archive is fixed, time-stamped and complete.   Verify, if necessary, the presence of a commitment from the editor of the cash register system to provide users and the tax authorities with the archiving data, particularly in the event that the user stops using the cash register system.
Functional verification   Check that the archiving functionality is available, that it provides archives in an open format and that the data present is time-stamped and complete.   Check that the cumulative period totals and perpetual totals frozen at each period are included in the archive.
Robustness check   Verify that the integrity and authenticity of the archive creation date data is protected by a robust mechanism, as described in Requirement 8.

---

[35] Open format: interoperable data format, i.e. independent of the software used to create, modify or read it, and whose technical specifications are public and without restrictions on access or implementation. *Article 4 of Law n° 2004-575 of 21 June 2004 for confidence in the digital economy*
[36] CF requirement n°7

Requirement 11: Archiving frequency
This archiving functionality must allow the user, at any date, to have access to or to be able to generate the archives for any past period of less than 7 years.   The period covered by an archive may not exceed one year or one fiscal year.
Examples of acceptable solutions
It is acceptable to give the user the possibility of defining the limits of the period for which he wishes to archive (while respecting the maximum constraint of one year/year) or to generate several periodic archive files (daily, monthly and/or annual).   Once the archives have been generated, it is the user's responsibility to keep them for the legal period of 7 years.   It is possible to give the user the option of accessing or generating archives for past periods longer than 7 years, but as the legal obligation to retain transaction data is limited to 6 years from the date of the last transaction of the fiscal year, it is also acceptable to provide this option only for 7 years.
Documentary audit
Check from the description of the archiving functionality that the user has the possibility to archive any desired period without exceeding one year or one fiscal year per archive.
Functional verification
Verify that the user can archive all the cash data for any desired period (in one or more files), at any date, but not exceeding the limitation of one year/year per archive.   For example, make one or more archives for a period of several days, 1 month, several months and/or 1 year. Check that it is impossible to make an archive file exceeding a period of one year or one fiscal year.

Requirement 12: Integrity of records
The data contained in the archive must be consistent with the original data in the cash register system and must provide a reliable mechanism, independent of the medium in which the archive is held, to ensure this integrity and to allow it to be verified, even after the user has stopped using the cash register system.

Specific note
If an archive is generated over a period of time that contains corrupted/deleted data in the system, this mechanism must detect this and highlight that some of the archived data is unreliable.
A taxable person who decides, for example, to change his cash register system or to stop using a cash register system is still subject to the obligation to keep his cash data for the statutory period[37]. To do so, he must keep the archives generated from the cash register system before he stopped using it. In the event of an audit by the administration, it must also be able to demonstrate that these archives are intact. The editor of the cash register system must therefore provide for the tax auditor to be able to verify the integrity of the archive data generated with his cash register system independently of it.
The security level of these mechanisms must be at least equivalent to that used to meet requirement 8.
Examples of acceptable solutions
For example, an archive can be secured by signature or key fingerprinting and stored on an external device (external disk, USB key, remote server, etc.).
The mechanism for verifying the integrity of the archive may, for example, be a tool that can be downloaded or accessed directly from the website of the publisher/manufacturer of the payment system. The publisher/manufacturer may also provide and commit to making it available on request.
Documentary audit
Verify that the mechanisms for ensuring the integrity of the archive are accurately described, including the cryptographic algorithms used.
Check that the manual for the tax authorities specifies how to access the means of verifying the integrity of the records and that its operation is correctly described.
Functional verification
Verify the presence of an archive integrity check and its effectiveness by attempting to modify the archive directly.
Verify, when generating an archive with corrupted data in the system, that the data in the generated archive cannot be confused with the data that is corrupted.
Verify that this means of verification is accessible even if the user has stopped using the cash register system.
Robustness check
Verify that the inalterability of the archives over time is based on a robust mechanism, guaranteeing a level of protection at least equivalent to that requested in requirement n°8.

IV.6) Purges

Requirement 13: Purge [38]
If the cash register system has a functionality to purge cash data due to the need to free up memory space, it must ensure that before purging is implemented, an archive containing all the cash data to be purged is generated and retained in accordance with requirement n°17. Cumulative and summary data must never be purged.

---

[37] CF requirement n°17
[38] BOI-TVA-DECLA-30-10-30-20250416: point 250.

Specific note
Only the deletion of data from the cash register system (responsible for storing the cash data in compliance with the requirements of this standard, and in particular 8 and n°n°16) before the end of the legal storage period[39] is considered as a purge. The conservation of archives then becomes the only way for a taxable person to keep his cash data for a possible tax audit[40]. Any deletion of data prior to the legal data retention period is not considered a purge operation and is not subject to requirements 13, 14 and 15.
Documentary audit
Check from the description of the purging method that it is systematically preceded by the generation of an archive containing all the cash data to be purged. If no purging procedure exists, check that this is described in the documentation.
Functional verification
Create an initial dummy archive containing a sample of original and modification data, copy this archive to another medium and then implement the purge procedure. Check the completeness of the archive generated by the purge against the initial archive.
Robustness check
Verify that the archive generated by this method is secured to the same level as requirement #12. Create an archive for a specific period. Perform a purge of the data for this same period. Check that the archive is consistent.

Requirement 14: Partial purge [41]
The purge functionality must not remove cumulative and summary data[42] and transaction tracking data[43] from the cash register system. This data must be kept[44] in the cash register system in a secure manner[45].

---

[39] CF requirement n°16

[40] CF requirement n°17

[41] BOI-TVA-DECLA-30-10-30-20250416: point 260.

[42] CF requirement n°7

[43] CF requirement n°15

[44] CF requirement n°16

[45] CF requirement n°8

Documentary audit
Check from the description of the purge method that the cumulative, summary and traceability data is always correctly stored, secured in the cash register system itself.
Functional verification
On a representative cash register system, input known data, perform a purge and verify the accuracy, and proper retention, of the cumulative and summary data for the purged period contained in the cash register system by comparing it with the data originally input.
Robustness check
Verify that the purge mechanism does not compromise the integrity of the cumulative and summary data maintained in the cash register system for the period for which the data has been purged.

IV.7) Traceability of operations

Requirement 15: Traceability of operations
The cash register system must ensure secure traceability of archiving, purging and restoration operations of application data by recording in the system, for each of these operations, its time stamp and the POS identifier from which the operation is made.
Examples of acceptable solutions
The traceability of these operations may be ensured by a secure event log or log book to the same level as defined in requirement 8. As "system" restores cannot be traced by the application layer, the data restores concerned are those performed from the application/cash register software.
Documentary audit
Verify from the description of the means to ensure the traceability of these operations that all archive generation, purging and data restoration operations are concerned by the mechanism.
Functional verification
After performing a set of archiving, purging and restoring operations on the data if necessary, check on the system: that it is possible to identify all the operations carried out; that a time stamp is set up; that an association exists between the operation and the device that performed it A change in traceability data is detected by the system.
Robustness check
Verify that the traceability data security mechanisms implemented are at least equivalent in terms of security level to the one achieved in requirement n°8. Verify that the time-stamping of operations is based on a reliable mechanism and that it is not possible to modify it.

IV. 8) Data retention

Requirement 16: Data retention
All the cash and traceability data, as well as proof of their inalterability, must be kept for 6 years (from the date of the last transaction of the fiscal year)[46].

---

[46] CF article L.102 B of the Book of Tax Procedures

Requirement 16: Data retention
Cumulative and summary data as well as traceability data[47] must be kept in the system[48]. The cash data (excluding cumulative and summary data and traceability data) can be stored either in the system itself or in the archive.
Specific note
The cash data concerned are all those defined in requirement n°3, the corrective data defined in requirement n°4, the test school mode data defined in requirement n°5, the cumulative and summary data defined in requirement n°7, the print/reprint traceability data defined in requirement n°9, the traceability data defined in requirement n°15 as well as the data defined in requirement n°18 for the traceability of POS data to the centralization system, if applicable. A taxable person who only retains the cash Z (cumulative total for the day) does not comply with its retention obligations. The verifications concerning the duration of data retention are based on a period of 7 years in order to simplify the possible interpretations of the Book of Tax Procedures and to take into account the exceptional cases of tax year shifts.   The system must be able to protect against physical failure of a storage medium or explicitly warn the user (subject) of his responsibility to retain his data in accordance with this requirement.
Examples of acceptable solutions:
For example, it is possible to implement processes and/or tools to supervise memory capacity, to estimate the necessary memory capacity, to warn the user of the need to perform a purge, to increase memory capacity if necessary or to redundantly store backups on physical media, if possible at a distance.
Documentary audit
Check from the description of the cash data retention method that all the cash data is retained for a period of 7 years.   Check for incoming payment data other than cumulative, summary and traceability data whether it is stored in the system or in the archive.   Verify that the editor has put in place measures to prevent the risk of memory saturation and that the system allows for data retention for at least 7 years.
Functional verification
Verify that the provisions put in place by the editor to reduce the risk of memory saturation are working effectively.   Check for incoming payment data other than cumulative, summary and traceability data whether it is stored in the system or in the archive.   Verify that cumulative, summary and traceability data are maintained in the system itself.
Robustness check
If data retention is provided by the system and not by the archive, check the ability of the cash register system to retain the cash data for 6 years.   Verify that this capability is based, for example, on the use of a mechanism that ensures the appropriate level of availability at the storage system level (hardware or software RAID-1) or at the file system level (redundancy of files on several storage units, logging and self-healing capability, etc.). Verify that the configuration of the mechanisms implemented ensures the proper preservation and availability of the cash data for 7 years.

---

[47] CF requirement n°15
[48] CF requirement n°14

Requirement 17: Retention of records
The archives must be kept in such a way as to guarantee the integrity and availability of the archived data in the event of an audit for a period of 6 years (from the date of the last transaction of the tax year).
Examples of acceptable solutions: Records may be kept within the cash register system, outside the cash register system, or by a third party archiver who is responsible for keeping the records. The necessary measures must be taken to guarantee the integrity and availability of the records in accordance with requirements 12 and 16.   The conservation of archives in the cloud is possible in compliance with the rules of art.
Documentary audit   Verify from the method of record keeping how the records are kept so as to ensure their integrity and availability with the same level of confidence as for requirements n°12 and 16.
Functional verification   Verify how records are maintained to ensure their integrity and availability with the same level of confidence as requirements 12 and 16.
Robustness check   Verify the ability of the cash register system to maintain records with integrity and availability with the same level of confidence as requirements 12 and 16.

Requirement 18: Centralizing system [49]
Where data storage[50] is provided on a centralized system, the cash register system shall provide a reliable mechanism for data transfer and ensure the completeness of the transferred data flow, including in the event of a current or past disconnection.   Disconnections and offline modes should be set to be used for a reduced duration.   The publisher must specify the maximum duration for using the system in offline mode.   The choice of the maximum duration must be documented and relevant taking into account the terms of use of the cash register system.   The user of the cash register system must be notified that the system operates in offline mode.

---

[49] BOI-TVA-DECLA-30-10-30-20250416: point 210.
[50] CF requirement n°13

Requirement 18: Centralizing system [49]

Specific note

A system is said to be a centralising system if one or more POS terminals which store the information locally before transmission transmit the cash data to a central system which ensures that it is kept in compliance with requirement no. 16 (this is the case for autonomous cash desks which periodically send back data or which send back data in real time while providing a buffer system in the event of disconnection).

On the other hand, a system with a client-server architecture where the client interface is only a graphical interface, without temporary data storage, which allows communication to a server (e.g. a web application opened in a browser) is not considered as a centralizing system insofar as the autonomous use of the interface without connection to the server is impossible.

If data retention in accordance with requirements 8 and 16 is ensured by the terminals, this requirement is not applicable.

The traceability of the cash data is aimed at ensuring that all the transaction data is correctly transmitted, even in the event of connectivity problems or transmission errors.

Examples of acceptable solutions:

In order to guarantee the completeness of the data transfer, it is possible to set up a time-stamped incremental numbering of the sent and received data or a reference to the last sent record (such as the record's fingerprint or signature), coupled with an identification of the source POS to ensure that no data is missing.

In order to guarantee the integrity of the transferred data, a signature, a key fingerprint, or a secure network protocol (such as TLS, IPsec) can be used.

If the system provides for the POS terminals to be able to carry out transactions autonomously in the event of loss of connection with the centralizing system, the locally stored data must have a level of security at least equivalent to that provided in response to requirement 8. In addition, when the connection is re-established, the centralizing system must ensure that it has recovered all data stored locally and temporarily by the POS terminals.

In the event of a loss of connection between the centralizing system and the terminals, it is acceptable for the centralizing system to identify which terminals are affected and since when (date/time), without exceeding the maximum duration proposed by the publisher.

Documentary audit

If data retention is provided by the terminals, check the evidence to demonstrate the inapplicability of this requirement.

If data retention is ensured by the centralizing system, check from the complete description of this system that the completeness of the data feedback is demonstrated. Verify that the publisher provides an explicit declaration of completeness of the cash data feedback.

Check the setting of the maximum duration of offline mode as well as the justification for this delay.

Check the documentation for the presence on the system of a means of informing the end user that it is in offline mode.

Functional verification

If data retention is provided by the terminals, check the evidence to demonstrate the inapplicability of this requirement.

Verify that a sampled set of cash data is correctly entered into the centralizing system.

Check the duration and causes of disconnections and offline mode.

Check the presence on the system of a means of informing the end user that he is in offline mode.

Check the identification of operations carried out in offline mode.

Requirement 18: Centralizing system [49]
Robustness check
In the case of encryption or signature of data shipments, verify that the level of security is at least equivalent to that provided in response to requirement No. 8.
Verify that all the cash data are stored and maintained on the centralizing system. Verify that a failure in the transmission of data or in the reception of data does not result in a lack of or erroneous data in the centralizing system.
Verify that the tamper-proofing mechanism is at least equivalent to the security level required to meet Requirement 8.
Verify that in the event of a loss of connection it is not possible to carry out transactions on the POS indefinitely and that the mechanism is sufficiently robust to ensure that all the elements are correctly reassembled when the connection is re-established.

IV.9) Tax administration access to the cash data

Requirement 19: Tax administration access to data [51]
The cash register system must provide access for the tax authorities to all [52] the recorded cash data. The publisher must provide an automated means for the tax authorities to verify the integrity of the cash data. The publisher must provide a user manual for the tax authorities, in French, detailing the procedure for accessing the data, as well as a clear description of the operation of the tools used to access the data and verify its integrity. This access must not jeopardize the security of the cash data.
Specific note:
The user manual for the tax administration must be clear and understandable to a non-IT specialist. It must also detail the procedure for checking that the data has not been altered.
Examples of acceptable solutions:
It may be possible to use the manager's account, or a dedicated administration account, to access all company data, which may be in native form (flat files, XML files, etc.) or in interpreted form for viewing purposes. The process of contacting and escalating to support can be detailed if necessary in the manual for the tax authorities. This can be included in the user manual or be a separate manual. The structure of the data presentation (the different fields) should be explicitly described. The user interface, menus, windows and other functionalities for the tax authorities can be described in the manual for the tax authorities. The manual for the tax authorities can be included in the generated archive.
Documentary audit

---

[51] BOI-TVA-DECLA-30-10-30-20250416: point 60 & 100.

[52] The data defined in requirement n°3, the corrective data defined in requirement n°4, the test-school mode data defined in requirement n°5, the cumulative and summary data defined in requirement n°7, the traceability data for printing/reprinting of receipts defined in requirement n°9, the data defined in requirement n°15 for the traceability of data purging, archiving and restoration operations, the data defined in requirement n°18 for the traceability of POS data transmission to the centralization system, if applicable.

Requirement 19: Tax administration access to data [51]
Check from the description of the tax authority's means of access that all the cash data is accessible. Verify the existence and relevance of the manual for the tax authorities describing the means and procedures for accessing the cash data. In the case of a cash register system with parameters allowing French compliance to be modified/activated/deactivated, check the presence of the fields, their values and the integrity of the settings so that the system complies with French regulations. Check the integration and security of offline mode settings.
Functional verification
Verify that the means of accessing the data for the tax authorities is functioning correctly and that all the cash data is accessible. Check that this means does not allow to modify or delete cash data. Verify that the means provided to the tax administration allows the correct detection of the alteration (modification, insertion, deletion) of data. For example, modify a data and verify that the detection of this error is easy and immediate by using the means of access of the tax administration. Check that French compliance parameters are attached to exports to the tax administration. Check the number of licenses identified for end customers in the license use case.
Robustness check
Verify that the administrative access does not compromise the security of the cash register system.

IV.10) Identification of the tax scope and major and minor releases

Requirement 20: Identification of the fiscal perimeter
The editor must clearly define the fiscal perimeter of his cash register system and list exhaustively all the source code files, libraries, drivers and modules impacting the functionalities and requirements stated in this standard.

Specific notes:
The source code files integrating the tax functionalities (security & inalterability, conservation, archiving, closing, school function, chaining or signing of data, access to the tax authorities, purging) must be listed and a print of these files will be taken in order to verify their non-modification.
If a portion of the tax scope is protected by a specific operating system configuration, the files in that configuration must have additional identification.
The non-tax scope is called "minor scope". The source code of the minor perimeter must be available to the evaluators during the robustness assessment in order to verify the consistency of the definition of the fiscal and minor perimeters.

Examples of acceptable solutions
The exhaustive definition of the fiscal perimeter can take the form of a correlation table between the 21 requirements of this repository and the list of all the source code elements involved.
For example, the tax scope includes all functions for recording the cash data; correcting/cancelling a transaction; functions related to recording and securing data generated by the school mode; closing functions (daily, monthly and annual); calculating, recording and securing cumulative and summary data; securing and inalterability of the cash data; securing receipts; archiving; securing archives; purging; traceability of operations (archiving, purging, closing); data and archive storage; access by the tax authorities and any other functionality/module/pilot/library that impacts compliance with the requirements of this standard.
It is possible to define the fiscal scope as the entire source code of the cash register system.

Documentary audit
Check that the list of components in the tax scope is complete so that the certification body and the publisher have no doubts about the portions of source code whose modification leads to a major version change.

Robustness check
Verify by source code analysis that all regulatory functionalities (i.e. related to the certification and the requirements of this standard) are implemented in source code files included in the tax scope.
Verify by sampling the source code that there are no regulatory features in the non-tax scope (minor)

Requirement 21: Identification of major and minor releases
The cash register system must be clearly identified by a major version number and a minor version number that are inextricably linked to the cash register system.
These version numbers must be easily accessible from the standard user interface of the POS system.
Any modification of the code in the fiscal perimeter or parameterization impacting the respect of the requirements of this standard must lead to an incrementation of the major version number.
The publisher must generate and provide the footprint of each major release.

Requirement 21: Identification of major and minor releases
Specific note:
The major version number of the cash register system is the identification of the version number of the tax scope of the cash register system.
The minor version number of the cash register system is the identification of the version number of the code not included in the tax scope and therefore does not impact compliance with the requirements of this standard.
If functions of the POS system can be disabled by specific settings, each function or variant must be identified separately.
The certificate issued by the BYCYB relates to the major version of the payment system evaluated and remains valid to attest to compliance with the conditions of inalterability, security, data storage and archiving for minor versions subsequent to the minor version evaluated by the BYCYB. It is possible to submit for certification a cash register system with fixed major and minor versions.
Examples of acceptable solutions
The following algorithms are state of the art to fingerprint software or software subparts for precise identification purposes: SHA-2, SHA-3, Whirlpool, Blake.
On the other hand, the following algorithms are not acceptable: SHA-1, MD5, CRC16, CRC32 and all other forms of non-cryptographic checksums.
It is possible to fingerprint versions from the binary or the source code. The fingerprint can be stored next to the source code.
The numbering format of major and minor versions is free. It is up to the editor to define and apply it.
In the case of systems that can be accessed directly by end customers (e.g. e-commerce), the display of the version number of the cash register system can be limited to a specific profile (e.g. tax controller or administrator).
Documentary audit
Verify from the documentation how the system identification by version numbers is created and how it is inextricably linked to the system itself. Verify from the documentation what measures are taken to protect the identification of the cash register system from tampering.
Check that the user manual describes how to display the identification of major and minor system versions from the user interface.
Verify that the naming rules for major and minor releases are clearly established and consistent with the requirement.
Verify from the documentation that the vendor has provided the major and minor version numbers of the cash register system being evaluated.
Functional verification
Check that the software identification is displayed as described in the documentation. Check that the identification presented is correct.

Requirement 21: Identification of major and minor releases
Robustness check
Verify that the mechanism used to generate the system identification via the major and minor version numbers has integrated all the parts of the system concerned and that it is reliable, i.e. that it follows the criteria of appendix B1 of the RGS, or, at least, that it is resistant to a collision attack (i.e. that it is not possible to forge two separate sources producing the same fingerprint).
Verify that the measures taken to prevent tampering are appropriate in relation to the state of the art.
Verify by sampling from the changelog or the code differential between two versions that minor changes do not impact compliance with the requirements of this Baseline.
Verify that a fingerprint performed by the evaluator on the certified code produces the same fingerprint as the one issued by the publisher.

Chapter V: Elaboration and validation of the reference system

V.1) Brand Committee

V.1.1) Modalities, role, and operating commitments

A brand committee of experts and various interested parties is formed to give an opinion on the certification rules.

The responsibilities of the brand committee are:

- give an opinion on the certification rules and their developments,
- give an opinion on communication or promotional action projects relating to the brand.
- give an opinion on the summary of all the controls and verifications carried out.

The brand committee meets at least once a year.

Any member of the committee undertakes:
- to contribute through its expertise to the proper functioning of the LNE cash system standard, to the development and updating of the reference framework established by BYCYB.
- to maintain the confidentiality of all information of an individual nature communicated to it, until its publication by BYCYB,
- to participate regularly in meetings, and if necessary to regularly inform his deputy and communicate the documents to him,
- to contribute to the development of BYCYB cash system standard, that is to say, to promote products or services certified under the brand.

The mandate of members is renewable by tacit agreement.

In order to preserve the credibility and effectiveness of the committee's work, BYCYB reserves the right to terminate the mandate of a member in the following cases:
- non-compliance with the confidentiality commitment,
- repeated absences from meetings without justification,
- non-compliance, in general, with the aforementioned commitments.

BYCYB ensures the animation and secretariat of the committee, and seeks the consensus of opinions of the members of the brand committee.

The exercise of the functions of member of the brand committee is strictly personal. However, in the event of absence, a substitute is designated and appointed under the same conditions as the incumbents.

BYCYB draws up the report of the committee meeting, highlighting the observations and proposals made, as well as any position contrary to the opinion issued by the committee. This report is sent to all members of the brand committee.

As part of the revision of this certification standard, BYCYB organizes the consultation and validation of the certification framework with in particular consultation of the DGFIP as a stakeholder.

V.1.2) Composition of the committee

The brand committee is made up of representation from interested parties associated with the certification of cash register systems. The list of committee members detailed below is indicative, not exhaustive and can be modified as necessary.
The LNE is an ex officio member of the committee.
The list of members of the brand committee is maintained and updated by BYCYB.
The committee is composed as follows:

Certification body:
• The representative(s) of BYCYB – Product and Information Technology Certification Department.

Certified organization:
• At least 3 representatives from cash register and invoicing editors.

Users:
• At least 2 user representatives.

V.1.3) Working Group

For the conduct of certain specific work, of a technical nature and not requiring the convening of all the members of the Trademark Committee, a working group may be set up, the members of which are designated by name and chosen from among those of the Trademark Committee. In the case of a working group, professionals or personalities from outside the committee may be called upon.

The tasks of this working group are specified by the Brand Committee; its remit will generally be limited to developing projects, proposals or providing additional information on a given subject on behalf of the Brand Committee.

V.2) Procedures for developing and validating the reference system

This standard was drawn up by BYCYB and approved by LNE.

It was drafted in accordance with the requirements of the law of 4 August 2008 and the decree of 19 December 2008 governing the certification of products and services. As such, and according to article L433-3 and following and R433-1 and -2 of the consumer code, the certification reference system is a technical document defining the characteristics that a product, a service or a combination of products and services must have, and the methods of checking compliance with these characteristics.

For the validation of this standard, BYCYB is responsible for :

- identify the relevant stakeholders;
- ensure the relevance of the selected stakeholders;
- to ensure that they are representative, without any one of them being predominant;
- to gather their views.

On the basis of feedback, the standard is reviewed by a specifically constituted brand committee, including all interested parties. It is approved using the same methodology as the first version.

V.3) Standards and reference documents

- Standard NF EN ISO 9001:2015 : Quality management systems - Requirements.
- Standard NF EN ISO 19600:2014 : Conformity management systems - Guidelines
- Law No. 2015-1785 of 29 December 2015 of Finance for 2016 - Article 88, amended by Law No. 2017-1837 Article 105
- Law n° 2004-575 of 21 June 2004 for confidence in the digital economy
- Consumer Code - January [1,] 2019 version - articles L433-3 to L433-11, articles R433-1 and R433-2
- General Tax Code - January [1,] 2019 version - Articles 286, 1770 duodecies
- Book of tax procedures - version of 1 January 2019 - articles L 16-0 BA, L47 A, L80 O, L96 J, L102 B, L102 D
- Order of 29 July 2013 amending the provisions of Article A. 47 A-1 of the Book of Tax Procedures relating to the standards for copies of files on computer media
- BOI-TVA-DECLA-30-10-30-20250416: Obligation to use certified software or cash systems
- BOI-CF-COM-10-80-20160803 : Right of access to various persons
- BOI-BIC-DECLA-30-10-20-40-20131213 : Preservation and representation of books, documents and accounting vouchers in the context of computerized accounting
- BOI-CF-IOR-60-40-20131213 : Control of computerized accounting
- General Security Reference System version 2.0 - Appendix B1 - Cryptographic mechanisms - version 2.03 of 21 February 2014

Chapter VI: Appeals and Complaints

VI.1) Appeals against decisions

The certification holder may contest the decision taken by letter with acknowledgement of receipt.

First, BYCYB re-examines the file in the light of the factual elements on which the appeal is based. It notifies the applicant of the decision or the new decision within 15 working days of receiving the appeal.

If the applicant wishes to maintain his appeal against the decision, he shall notify BYCYB by registered letter with acknowledgement of receipt within 15 working days. This appeal, which does not suspend BYCYB's decision, must be substantiated. It is examined by BYCYB within 21 working days of receipt and, where it concerns the certification decision, is examined by the reading committee. BYCYB informs the appellant whether or not its decision is upheld.

If the appeal is upheld after investigation and submission to the Mark Committee for an opinion, the appeal is presented to BYCYB's Certification and Impartiality Preservation Committee, which, after examination, proposes its conclusions. The final decision is notified by BYCYB to the Company.

Any subsequent dispute may be submitted to the competent Ministry of Industry or is brought before the competent courts.

VI.2) Handling of complaints

Any complaint concerning products is examined by BYCYB to confirm whether the complaint actually concerns certified products. The entity making a complaint must support it with factual evidence.

On receipt, BYCYB examines them and, if necessary, contacts the company concerned.

The company concerned must then inform BYCYB of the action taken and keep records of the complaint and the action taken to resolve it. Verification of the implementation of the announced actions may be the subject of additional examinations at the Company's expense.

As part of the Enterprise's monitoring, BYCYB examines the records relating to complaints and claims and checks that the appropriate corrections and corrective actions have been taken.

Chapter VII: Annexes

VII. 1) Lexicon

Archiving	The purpose of the archiving functionality, intended for users, is to export, by guaranteeing the date of creation of the archive, the frozen cash data in an open format in order to protect against the loss of data following a hardware problem, a security breach, or a change of the cash register system. It should not be confused with just a long-term data backup solution. It is a means for the taxpayer to be able to keep his cash data independently of the cash register system and to be able to communicate them to the tax authorities in case of an audit.
Archive	An open format file generated by the archiving functionality containing the incoming payment data for a defined period. The archive may not contain cash data for a period longer than one year or one fiscal year.
Authenticity	A characteristic of a piece of data for which the system is able to verify the identity of the author. It can be ensured through key fingerprinting or signature mechanisms.
Chainage	An algorithm that makes the proof of integrity of one piece of data dependent on the proof of integrity of the previous piece of data, thus constituting a proof of the integrity of the entire data set. This mechanism does not guarantee the integrity of the last element and does not allow counting the number of missing elements (links) when the chain is broken. The integrity proof can also be a proof of authenticity to additionally guarantee the authenticity of the chain.
Coding	Financial valuation, or the act of writing or transcribing in numbers. Not to be confused with encryption.
Encryption	A cryptographic mechanism for ensuring the confidentiality of data, using a cipher (in the sense of a secret code). Data encryption is not required by this repository. Not to be confused with encryption.
Private and public keys	A digital signature is generated from a private key, which is a cryptographic secret, and a document to be signed. The verification of a signature is made from the original document and the public key associated with the signer. Knowing a public key does not allow to find the corresponding private key.
Fence	Functionality, either manual or automatic, offered by the cash register system that aims to close a daily, monthly or annual period, i.e. to make it impossible to record new transactions, to change or cancel a transaction over a closed period.

Privacy	A characteristic of information or a system that ensures that access to it is strictly limited to authorized persons. Confidentiality is not required in the context of the repository. It can be ensured through encryption.
Encryption	To insert or hide a hidden meaning in a text or statement, intentionally or not. Example: "deciphering a political speech". For the anglicism, see encryption.
Cash data	The cash data corresponds to all the data defined in requirement n°3, the corrective data defined in requirement n°4, the test-school mode data defined in requirement n°5 as well as the cumulative and summary data defined in requirement n°7 and the traceability data for printouts and reprints of receipts defined in requirement n°9
Basic data	Data that is not obtained by calculation from other data. Any elementary data that contributes to the constitution of an accounting entry, to the justification of an event or a situation transcribed in the books, registers, documents, vouchers and declarations is covered by the right of control of the tax authorities.
Publisher	The person who owns the source code of the cash register system and who has control over the modification of the parameters that impact the conditions of security, conservation and archiving of the cash data of the system.
Fingerprint / hash / condensate	The result of a function that associates to a data of arbitrary size a data of fixed size. When the fingerprint is of cryptographic quality, it is not feasible to calculate the inverse of this function.
Key impression	A cryptographic fingerprint made by combining the source data with an authentication secret. This ensures that only the holder of the secret can generate and verify a fingerprint. A key fingerprint guarantees the integrity of a document and ensures its authenticity, without being able to distinguish the identities of the secret holders.
Checkout functionality	Functionality that consists in memorizing and recording extra-accountably payments received in return for a sale (of products or services). If the payment triggers concomitantly, automatically, obligatorily, instantaneously and without human intervention the posting of an accounting entry, the functionality is not considered as a cash functionality but as an accounting entry functionality.
Timestamp	A single monotonically increasing time value indicating the date and time at which an event occurred. This data is presented in a consistent format, making it easy to compare two different records and trace them back in time.
Accountability	The possibility of attributing responsibility for an act to a person.
Unalterable	The characteristic of a system where nothing can change the recorded data without traceability (i.e. without the system detecting it). An alteration of the data constitutes a breach of its integrity and authenticity.
Integrity	A characteristic of data that has not been altered or destroyed, either intentionally or accidentally.

Logging	Sequential recording of events affecting a particular process. It is a means of ensuring the traceability of events.
Supporting document / voucher	A document containing data to justify the details of the order, sales, purchases and method of payment for a product or service.
Billing software	Computer system enabling invoices to be issued between taxable persons for VAT purposes, containing the compulsory information provided for in Article 242 nonies A of Annex II to the CGI and complying with the conditions of Article 289 of the CGI
Free software	Software that users are free to use, study, modify and distribute. These freedoms allow users to adapt the software to their specific needs. Source: BOI-TVA-DECLA-30-10-30
Agent	Legal or natural person established in the European Economic Area (E.E.A.) who has a function of representation of the holder outside the E.E.A. and has a written mandate of this one signifying that he can act in his name in the process of certification according to the provisions of these rules. The representative can also be a distributor or importer of the certified products, his different functions are then clearly identified.
Mode/school environment/test	An optional mode or environment of a cashiering system for generating or simulating data to record fictitious transactions for testing or training purposes.
Fiscal perimeter	The complete set of source code, libraries, drivers and modules that impact the functionality and requirements stated in this repository.
Proof of authenticity	A data element that can be used to prove the authenticity of a document. See key impression, signature.
Proof of integrity	A data element that can be used to prove the integrity of a document. See imprint, signature.
Purge	Irreversible deletion of data stored on a system.
Redundancy	A method consisting of duplicating all or part of the data in order to be able to restore it to its original state in case of alteration. It can ensure the availability of information, which is the capacity of a system to remain functional or to keep data accessible over time.
Cryptographic secrecy	A cryptographic secret is a confidential data used to encrypt or authenticate a document. The confidentiality of this secret guarantees the properties (confidentiality or authenticity) of the mechanism that uses it. To qualify as cryptographically secure, the secret must be randomly generated, not be used for different purposes, and have a size defined by the mechanism that uses it.
Signature	A digital signature is a mechanism to guarantee the integrity of a document and ensure its authenticity. Unlike a key fingerprint, the verifier does not need to know a secret to verify authenticity and cannot impersonate the signer.

Cash register system	A cashiering system is a computer system with cashiering functionality.
Holder	Legal entity that ensures the control and/or the responsibility of the respect of all the requirements defined in the present certification rules. These requirements cover at least the following stages: design, manufacture, assembly, quality control, marking, packaging as well as the placing on the market and specify the critical points of the various stages. Some of these activities may be carried out on the holder's site or on another site by the holder himself or by another structure with which there is a delegation of responsibilities. This includes for example subsidiaries or subcontractors. Whatever the site or the level of outsourcing, it is important that the holder is able to present all the evidence of compliance with the standard. Paragraph 310 of BOI-TVA-DECLA-30-10-30-20160803 indicates that the holder is the publisher of the cash register system. If the holder is not established in the European Community, he must appoint an agent.
Cumulative total / period-to-date	Cumulative sales settled since the opening of the period in question. This is a counter that is initialized to 0 at the opening of the period (or closing of the previous period) and whose value is stored at the end of the period.
Total perpetual / cumulative perpetual	Cumulative turnover counted since the cash register system was initialized. This is a counter that never resets, that is not directly linked to a period but whose value is recorded at a given time: at the time of each closing (daily, monthly or annually).
POS	Point of Sale terminal identified by a unique number (terminal number, cash register number, scale number, etc.). A terminal ensures the recording of the cash data locally, temporarily (pending the transfer of data to a centralized system) or in compliance with requirement no. 16 concerning the retention of data for a period of 6 years from the date of the last transaction recorded in the current fiscal year.
Traceability	Ability to trace the history, implementation or location of what is being examined. It is related to logging and accountability.
X	Term from the old key-operated cash registers. Simple reading of the day's turnover, which can be done at any time and without impacting on the recorded transaction data.
Z	Term from the old key-operated cash registers. Closing the cash register for the day: no more changes can be made to the transaction data recorded since the last Z, only the cash balances (e.g. the cash still in the cash drawer) are retained.