Vol.49, Special : pp. 115-120, January 2006
ISSN 1516-8913 Printed in Brazil

BRAZILIAN ARCHIVES OF
BIOLOGY AND TECHNOLOGY
A N I N T E R N A T I O N A L J O U R N A L

The Control of Documents Maintained in The Electronic Media and the Requirements of NBR ISO/IEC 17025 and Adequacy for PNQ

Anselmo Ferreira de Castro[1], Glória Maria Pereira da Silva[1], Stella Regina Reis da Costa[2], and Sílvio Francisco dos Santos[1*]

[1]General Accreditation Coordination; Inmetro - Cgcre/Inmetro; Rio de Janeiro - RJ - Brasil. [2]UFF/UFRRJ; Rio de Janeiro - RJ - Brasil

ABSTRACT

During the assessments carried out by the authors at the diverse laboratories pertaining to the network of accredited laboratories - known as the Brazilian Calibration Network (RBC) - the authors verified the difficulties that these laboratories had in meeting the requirements of NBR ISO/IEC 17025:2001 (Standard), related to the maintenance of documents in the electronic media. More and more laboratories are substituting traditional control with electronic document control, which allows for more agility in the recovery of information. These laboratories implement policies and procedures; however, they still feel insecure, in some way, as to how to meet all of these requirements, thereby giving rise to difficulties in the implementation of such. The aim of this paper is to discuss the control of documents stored in the electronic media, adopting requirement 4.3 of the Standard as the reference, and aiming, in this manner, to harmonize the assessment process of the procedures of document management in the electronic media, and to assist the laboratories in the interpretation of the Standard, so that they may implement systems that are adequate to their actual necessities and to their structural size, while at the same time complying with the referred to requirement. This work will not broach the treatment given to the records (requirement 4.12 of the Standard), facts (requirement 5.4.7) nor to the electronic transmission of results (requirement 5.10.7), leaving these subjects for posterior discussions.

Key words: NBR ISO/IEC 17025, PNQ, computerized systems, documents

INTRODUCTION

At the moment, the great majority of laboratories make use, to a greater or lesser degree, of computerized media in order to store their documents. Among the advantages of computerized control is the possibility of increasing the productivity and competitiveness of the laboratory.

Among the activities of the internal and external auditors, as well as of the assessors from Cgcre/Inmetro [3, 4 e 10], is the assessment of the adequacy and implementation of the policies and procedures adopted by the laboratories, for document control. The adequate implementation of this aspect is one of the essential factors for the demonstration that the laboratory is competent, as specified by the Standard.

According to Coutinho et al. (2004), in a comparative study of the nonconformities

* Author for correspondence

identified by the accreditation bodies belonging to the American Association for Laboratory Accreditation (A2LA) and to those belonging to Cgcre/Inmetro, requirement 4.3 of the Standard - *document control*, is responsible for 8,2% of the nonconformities reported by the A2LA and for 10% of the nonconformities reported by the Brazilian body. Coutinho's sample involved the consideration of the reports of all the assessments carried out between 2001 and 2003. In both cases, document control was the third biggest cause of nonconformities.

During the assessments, it was observed that among the difficulties of the laboratories, is the understanding of the requirements of the Standard, as well as of some of its concepts, in particular, the definition of document, and what the importance of its control for the maintenance of a "traditional "or computerized quality system is.

Although they may seem simple, we believe that the knowledge of such concepts is fundamental to the initiation of our discussion.

The definition of a document

NBR ISO 9000:2000, in the part that deals with fundamentals and vocabulary, defines a document in the following manner:

*"A **document** is the information and its supporting medium."*

In the ABNT ISO/GUIDE 2:1998, note 2 of item 3.1, considers the term "*'**document**' as being any medium that contains registered information*". Note 3 of the same item considers "*the document and its content as being a single entity*".

The Standard presents the following as examples of documents: regulations, standards, calibration and/or testing methods, drawings, specifications, instructions, manuals and software. The documents may be contained in various media: electronic, on paper, and may be digital, analogical, photographic and written.

The 17025 does not present a definition of an electronic document. A definition accepted by the authors deems "an electronic document as being that which is memorized in a digital format, and which is not perceptible to the human eye without the intervention of a computer"[6].

In a general manner, we can consider all information stored on an electronic device (hard disk, floppy disk, CD-ROM) or transmitted through electronic means, to be an electronic document. In this context, software, data bases, texts, images, as well as the information accessed via the Internet: e-mail, websites etc. may also be included.

Some laboratories opt to maintain their documents on paper, while others only use the electronic media, and yet others maintain "a hybrid" form, wherein both paper and the electronic media are used.

The importance of document control

The importance of document control, both for those documents which are generated internally and for those which are obtained from external origins, resides in the need to identify the personnel authorized to review and approve of such documents, in the identification of the status of their revision and in the identification for distribution to those who have access to such documents. Another characteristic of document control is that it should be capable of making documents readily available, as well as of avoiding the use of invalid and/or obsolete documents.

A system of document control must be able to generate, issue, receive, store or process information in some other manner, while at the same time trying to maintain the integrity of the documents. These aspects are assessed in item 5.1, Management of the Information of an Organization, of Criterion 5, Information and Knowledge, of the management model for excellence called for by the National Quality Prize (PNQ).

METHODOLOGY

In this paper, we will begin by presenting some considerations with regards to electronic documents, and some of the characteristics of such documents. We will then revise requirement 4.3 of the Standard and Criterion 5.1 of PNQ. This will be followed by a discussion and an interpretation of these requirements as applied to electronic documents, suggesting an approach for the assessment of these requirements, which is of fundamental importance for a quality system to function well. Finally, we will draw a conclusion with regards to the discussion.

CONSIDERATIONS

For the documents maintained in the electronic media, we consider the definitions contained in NBR ISO/IEC 17799:2001: Information Technology - Code of Practice for Information Security Management as being valid. This document deals with the management of information security and applies the following definitions:

– Confidentiality: ensuring that information is accessible only to those authorized to have access;
– Integrity: safeguarding the accuracy and completeness of information and processing methods;
– Availability: ensuring that authorized users have access to information and associated assets when required.

Bearing the approach and the application of the criteria on information and knowledge in mind, the following practices are requested for the markers that make up item 5.1:

– How are the necessities of systematized information identified in order to support the daily operations and the taking of decisions on all levels and in all areas of the organization?
– How are the main information systems defined, developed, implanted and updated, aiming at meeting the identified necessities?
– How is the necessary information made available to the users?
– How is the integrity, the updating and the confidentiality of the information that is stored and made available assured?

In order to work with electronic documents, we need to understand the mechanism of the electronic signature. This technology tries to overcome the purposes of traditional signatures, and it is obviously not the copying and pasting of a scanned signature onto an electronic document, but rather a system of codes to identify and authenticate the authors, that is dealt with by software.
Depending on the type of security system used, there are basically two types of electronic signatures: *passwords and public keys*.

For our purposes, passwords offer the necessary level of security, which is many times greater than that which is offered by paper. For this reason, we will not deal with public keys here.
It is necessary to point out that the aim of the electronic signature is not to make the document illegible, as the content itself is not encrypted, but rather to increase the state of security of the signed document, in such a way so as to guarantee its confidentiality, integrity and availability.
The operational systems offer some options of access control through passwords. Among the resources offered by such software are:

1. A password to access the network environment;
2. A password for the sharing of resources. In this case, there are two types of access control: access control at the level of sharing, which allows one to supply access to each shared resource (for example: folders and printers) and access control at the level of the user, which allows one to specify which users or groups may have access to each shared resource;
3. A password to protect the computer during waiting periods;
4. A password to protect the screen.

DISCUSSION OF THE REQUIREMENTS OF THE STANDARD WITH REGARD TO DOCUMENT CONTROL

For the control of documents maintained in the electronic media, we shall discuss the following items (the numbers in parenthesis refer to the items of the Standard relative to document control):

a) The laboratory shall control all the documents that form part of the quality system (4.3.2.1)
The laboratory defines, in accordance with the Standard, how, and in what medium it shall keep its documents.
It would be apt, in this requirement, to observe the systematic orientation adopted by the laboratory in order to control the documents of external origin as, generally speaking, some laboratories forget to deal with such issue.
The access to documents maintained in the electronic media - internal or external - can be

made through a reference (link, bond). This systematic orientation is extremely useful, as it reduces the possibility of using obsolete documents.

If the laboratory keeps a printed copy of a document, or a copy in one of its computers, it would be advisable for them to present the systematic orientation that guarantees that the latest valid edition of the document is being used, in such a way so as to avoid the revision being kept within its system from being different to that being kept at the original source of such document.

b) All the documents which are issued for the laboratory personnel as forming part of the quality system must be reviewed and approved for use by authorized personnel, before being issued. A master list or equivalent procedure should be established, that identifies the status of the current review and the distribution of the quality system documents.

The laboratory should have evidences of all the reviews carried out on its documentation available, whether the document has been revised or not.

One of the characteristics of electronic control is the creation of a spread sheet (master list or equivalent procedure) wherein the data that identifies the quality system documents is given. The quick localization of documents helps make the services offered by a laboratory become more efficient.

It would be advisable for the document control procedure to contain, at the very least, the following information:

1. Definition of responsibilities for elaboration, approval and revision;
2. Systematic orientation for the issuance and revision of documents;
3. Systematic orientation for access, protection and backup.

It would be advisable for the master list to contain, at the very least, the following information:

1. Document link/path/address
2. Title of document
3. Revision number
4. Date of revision.

In order to meet the characteristic of confidentiality, it is advisable for the laboratory to define the initial date on which the passwords become valid. Traditional documents shall function in the same manner: from the moment in which a person assumes a position or function, s/he shall be held responsible for those activities which have been attributed to him/her.

c) It must be assured that authorized editions (for example, by password) of appropriate documents are available at locations where essential operations are carried out (4.3.2.2 a).

The printing out of a non-controlled copy, and the use of a laptop, CD, floppy disc etc. is acceptable, as long as the use of the latest valid revision is assured.

Attention must be paid to the systematic orientation adopted for the case in which the laboratory carries out activities outside its permanent installations. That is, how the laboratory makes the documents available in such cases, and how it assures that the valid editions are used.

d) It must be assured that invalid and/or obsolete documents are removed from all the points of emission and use, or that their unintentional use is impeded (4.3.2.2 c e d).

e) It must be assured that all the quality system documents generated by the laboratory are unequivocally identified (4.3.2.3).

It is understood that the documents may be kept in the electronic media in a partial manner, however, when they are presented to clients, for example during audits etc., they must be preserved in the format in which they were originally produced, and they must be interpreted in the context in which they were meant to be used;

f) The identification should include the date of issuance, and/or identification of the revision, the page numbers, the total number of pages or a mark identifying the end of the document and the issuing authority (4.3.2.3).

The identification of the issuer can be made through the definition of the access control. In this case, only the issuers (or predefined people) have permission to issue documents for which they are responsible. Such permissions may be granted to a user (access control at the level of a

user) or to a group (access control at the level of sharing) through passwords. The adequate use of passwords is of fundamental importance, as they are intended to meet the same needs as traditional signatures, and are one of the forms of an electronic signature. Once a person has valid access, s/he acquires legitimacy to carry out actions restricted to authorized personnel;

g) The alterations to the documents shall be reviewed and approved by the same function that carried out the original review (4.3.3.1).
See items ***c*** and ***i***;

h) The altered text, or the new text, shall be identified in the document or in an appropriate annex (4.3.3.2).
See item ***i***;
Attending to items *a* to *h* guarantees the adequacy of markers *a.1, a.2* and *a.3* of item 5.1 of the PNQ assessment instrument.

i) To assure confidentiality, the procedure adopted by the laboratory should establish a systematic orientation that defines who has access to confidential information (4.1.5 c).
It would be advisable for the laboratory to define, specifically, which documents the people are authorized to access. The use of an individual password can be an adequate mechanism.

The available software offers systematic orientations to restrict access to documents. Such systematic orientations involve:

1. Attribution of a password to open documents, thereby avoiding unauthorized users from accessing them (*protection password*);
2. Attribution of a password for the modification of documents, which allows other people to access the document, but not to alter it in any way without the password. If a person were to access the document in order to modify or alter it without the password, s/he would only be able to save the document by giving the file a different name (*protection password*);
3. Recommendation that others may open the documents as a reading-only file. If a person were to open the document as a reading-only file, and alter it, s/he would only be able to save it by giving the document a different file name. If the person opens the document as a reading-writing file, and alters it, the document could be saved using its original file name;
4. Attribution of a password when a document is sent for revision, which prevents alterations from being made, except for commentaries or controlled alterations;
5. Attribution of a password in order to use areas of a form, in order to create forms, which will avoid others from altering the specified sections;
6. Attribution of a password to protect working folders and spread sheets from being altered;
7. Attribution of a password to protect spread sheet cells, graphic data etc.

It would be advisable for the laboratory to have a systematic orientation for the attribution of passwords in such a way so as to avoid problems which may occur due to employees forgetting or leaving the organization, for example.
It would be advisable for the laboratory to establish backup procedures that assure the protection and the safe storage of information, demonstrating which measures are adopted to prevent losses and, whenever possible, the backup documents should be stored outside the laboratory's installations.
It is difficult to make safety copies of paper files, while it is easier to implement a backup procedure for electronic files. However, a critical point in this in case is the control of versions. When a document is altered, this altered version is made available as the most recent version. An inverse *backup* is normally provoked when a previous version has to be consulted, and this should be avoided. In fulfilling item ***i***, it is possible to attend to marker a.4 of item 5.1 of the PNQ, in which refers to electronic documents.

CONCLUSION

We have verified that the treatment to be given to the control of electronic documentation, saved in their due proportions, is not very different from the treatment adopted for those documents kept in a physical format.
The maintenance of documents in the electronic media offers many advantages, including: agility, speed and security, both for the organization's internal staff members as well as for its clients.
At present, the main disadvantage of using the electronic media for document control lies in the connection that such media has to technology. In order to overcome this, the laboratories have to maintain the equipment and the software necessary

for the recovery and the exhibition of the filed data, during the time period in which documents have to be retained.

For there to be success in this modality of document use, it is necessary to apply 17025 correctly, paying attention to the confidentiality, integrity and availability of information, which naturally leads to compliance with item 5.1, Management of the Information of an Organization.

During the internal and external assessments and audits, the size of the laboratory and the degree to which it is computerized must be taken into account: as in all activities, the use of common-sense is a fundamental factor for the success of these activities.

We would like to point out that it is up to the laboratory to establish and to decide upon the best systematic orientation, which is adequate for the Standard, and which is appropriate for its circumstances.

This discussion should not be interpreted as an additional requirement, nor should it be used as an integral part of the Standard.

ACKNOWLEDGMENTS

We would like to thank the collaboration of the staff members of Cgcre/Inmetro, who contributed to the realization of this paper.

REFERENCES

[1] NBR ISO/IEC 17025 - *General Requirements for the Competence of Calibration and Testing Laboratories*.

[2] DOQ-CGCRE-002, Rev. 00 - *Orientations for carrying out internal audits and reviews on calibration and testing laboratories* - Inmetro (www.inmetro.gov.br).

[3] DOQ-DQUAL-006 - *Orientations for the adoption of NBR ISO/IEC 17025 by accredited laboratories and by laboratories awaiting accreditation*. Disp. in: http://www.inmetro.gov.br.

[4] NBR ISO 9000:2000 - *Quality management systems - fundamentals and vocabulary*.

[5] ABNT ISO/IEC GUIDE 2 (1998), *Standardization and related activities* - General vocabulary.

[6] Gandini, J. A.; Salomão, D.; Silva, D. P. and Jacob, C. (2004), The s*afety of digital documents*. (*A segurança dos documentos digitais.*) Available at: http://www1.jus.com.br/doutrina. Access in: 13 Jul. 2004.

[7] Coutinho, M. A. O. (2004), *Implementation of the requirements of the NBR ISO/IEC 17025 Standard in laboratories: a proposed set of actions to reduce the incidence of nonconformities in the processes of granting and maintaining accreditation by Cgcre/Inmetro*. (Implementação dos requisitos da Norma NBR ISO/IEC 17025 a laboratórios: uma proposta de ações para reduzir a incidência de não conformidades nos processos de concessão e manutenção da acreditação pela Cgcre/Inmetro.) Master's Degree Dissertation on Management Systems at the Federal Fluminense University (Universidade Federal Fluminense) - UFF.

[8] *UNCITRAL Draft Model Law on Electronic Commerce*. (2004), Available at: http://fletcher.tufts.edu/multi/texts/uni.txt. Access in: 15 Jul. 2004.

[9] Santos, S. F.; Follador, A. C.; Diniz, M. and Soares, M. A. (2003), Methodology for the auditing of laboratory quality systems in accordance with NBR ISO/IEC 17025. (Metodologia para auditoria de sistemas da qualidade de laboratórios segundo a NBR ISO/IEC 17025). In: 2003 Metrology Congress - Metrology for the Life of the Brazilian Metrology Society. (Congresso Metrologia 2003 - Metrologia para a Vida da Sociedade Brasileira de Metrologia). *Proccedings...*

[10] NBR ISO/IEC 17799 (2001), *Information Technology* - Code of Practice for Information Security Management.

[11] Criteria of Excellence of the Foundation for the National Quality Prize (2005), São Paulo: FNPQ. Available at: http://fnpq.org.br.

Received: July 29, 2005;
Revised: September 05, 2005;
Accepted: November 22, 2005.