Certifying the Quality & Information Security Management Systems of the NSO according to the international standards ISO 9001, 20252 and 27001

Segui, Federico
National Statistical Institute, Quality Management Department
Rio Negro 1520
Montevideo (11100), Uruguay
E-mail: fsegui@ine.gub.uy

Introduction

On January 22nd 2009, NSI [1] of Uruguay obtained a quality certification according to the international standard ISO 20252:2006 "Market, opinion and social research – Vocabulary and service requirements". It establishes quality service requirements of statistical producers, either official ones or business enterprises.

NSI of Uruguay is the unique national statistical office which gets this certificate (ISO 20252) - no information known about any other realisation so far. Furthermore, it achieved simultaneously two certifications of its Quality Management System (QMS), in accordance with international standards ISO 9001:2008 and ISO 20252:2006.

A pilot experience in the Construction Cost Index (CCI) survey was the starting point of a bigger project that has already started and involves all NSI areas. Documentation, standards, politics and know-how were produced and will be used in other surveys in an easy way and at a lower cost.

The implementation of the information security management system (ISMS) according to the international standard ISO/IEC 27001 into the Continuous Household Survey started at the end of 2010 as a pilot experience. It has been supported by the technical assistance of the Agency for e-Government and Information Society (AGESIC initials in Spanish) of Uruguay.

Antecedents

There are many quality frameworks and QMS models like ISO 9000, EFQM [2], TQM [3], DQAF [4] or a combination of them being used in statistical offices.

Handbook on "Data Quality Assessment Methods and Tools" has been one of our main references during planning phase of our implementation plan. It describes in detail each quality framework available.

NSI of Uruguay has adopted the ISO 9000 model because there are some employees trained as ISO 9000 QMS experts. Some of them are Certified Consultants by ISO subsidiary in Uruguay and experienced in ISO certifications in private organisations.

ISO 9000 norms are widely-known international standards that establish guides and requirements of a Quality Management System (QMS) in any kind of organisation. They have been studied and exposed in many other papers and publications before, so we shall proceed to the next subject.

ISO 20252 is a Process Quality Standard that is specific to the carrying out of survey research *[Blyth, Bill 2006]*. It does not cover issues of design quality because it is almost certainly impossible to define by consensus what composes good design quality. Furthermore, this is a global standard suitable for use in any statistics production organisation, so dealing with design quality, cost and timeliness to provide fitness for

1 NSI – National Statistical Institute or National Statistical Office (NSO)
2 EFQM – European Foundation for Quality Management
3 TQM – Total Quality Management
4 DQAF – Data Quality Assessment Framework – International Monetary Fund

purpose may vary from one organisation to another. The core content is: QMS requirements, executive elements, data collection, data management and processing, project documentation.

The international standards ISO 27000 are a group of norms focused on information security management systems. The term *information* includes all forms of data, documents, communications, conversations, messages, recordings, and photographs. The goal is to protect the information assets of the organisation. Asset is defined as "anything that has value to the organisation" and information asset is "knowledge or data that has value to the organisation" [ISO 2005].

Some benefits of implementation of the information security management system according to ISO 27001 are: information security is an integral part of the organisation's whole management system; the main factors affecting efficiency and effectiveness in the organisation, information and its security are in a controlled mode; reliability of the system is supported by back-up systems; employees are responsible for information security of their workplaces as well as of their users/customers; a requirement for a continual improvement guarantees an efficient control of costs in the long run.

ISO 9001 or ISO 20252? Both standards are not exclusive, but they are complementary. In fact, ISO 9001 certification has facilitated ISO 20252 certification process at NSI of Uruguay. Furthermore, ISO 9001 and ISO 27001 have in common the implementation of very similar management systems, one of them oriented to quality and the other one focused on information security, but the core of both management systems is the same. We strongly recommend implementing the two or even three standards at the same time.

Organisational structure

A Quality Management Department has been created during a project of organisational restructure.

QM Dept. depends on Director General Office and it is an independent Department that works like an advisory and support office.

It is strongly recommended to create working groups (quality committee and information security committee) leaded and moderated by the Head of Quality Manager Department and integrated by key employees inside the organisation. Top Managers and those employees who have natural leadership qualities and big influence on their fellows, even if they do not have a management position.

The quality working group is responsible for proposing continuous quality improvements and establishing the action plan for the implementation of ISO 20252. Whilst the information security committee has the commitment of implement and maintain the information security management system through establishing policies, procedures, guidelines and controls in order to eliminate, minimize or accept the risks associated to each information asset.

Pilot experiences

A quality improvement project started on February 2008, when NSI decided to begin a pilot experience in a small survey (Construction Cost Index, CCI). This pilot project was developed in a record time of about 10 months. On November 2008 CCI survey was ready to ask an external audit to certificate its QMS according to ISO 9001:2008 and ISO 20252:2006 standards. LSQA (associated to Quality Austria) was the accredited organisation contracted [5] to lead the certification audits.

Beginning by a pilot project in a small survey gives us all necessary feedback to make adjustments and generate know-how to implement easily the ISO 20252 into all NSI surveys.

Regarding to ISO 27001, on September 2010 began a project to implement an information security management system into the Continuous Household Survey as a pilot experience.

Implementation plan

We have developed an implementation plan whose success was truly proved into the pilot experience during 2008. This plan is currently used to implement a QMS into five statistical operations. Key features of

[5] Selected by public bidding

the implementation plan are exposed as follows:

Annually NSI spends about 100 hours of quality training. Basically, training activities are: workshops on Quality in Statistics for all staff involved; courses of Introduction to ISO 9000 and ISO 20252 standards specially designed for quality facilitators and Course of Quality Management for managers.

Initial situation diagnosis was conducted based on DESAP [6]. The questionnaire was filled not like Eurostat proposes, but the answers were discussed and accorded by consensus into all survey staff. It helped to integrate people, transfer know-how between them and give different points of view about the survey issues.

A SWOT [7] analysis was done based on DESAP results and evaluations from survey employees.

Evaluation about gap between initial scenario and ISO 20252 requirements was followed up to make adjustments into the implementation plan.

Define and plan the implementation of the Information Security Management System (ISMS) according to ISO 27000 means: to establish the scope and boundaries of the ISMS; define NSI's ISMS policy and the approach to risk assessment; identify information assets and security risks; analyse and evaluate that security risks; identify and evaluate risk treatment options and actions; select control objectives and controls to treat risks; make sure that top managers formally approves all residual risks (those that are left over after implement the risk treatment decisions); get authorization from top managers before implement and operate NSI's ISMS; prepare a Statement of Applicability that lists NSI's specific control objectives and controls.

In order to implement and operate the NSI's ISMS is necessary: to develop a risk treatment plan to manage information security risks; implement risk treatment plan, security controls and training programmes; manage and operate the ISMS; manage ISMS resources; implement security procedures.

Maintain and improve the ISMS require: to implement ISMS improvements; take appropriate corrective and preventive actions; apply the security lessons that the NSI have learned; communicate ISMS changes to all interested parties; make sure that ISMS changes achieve the intended objectives.

Quality Indicators & Reports

The Quality Indicators have been defined mainly based on Eurostat's SQI. In fact, they are a linkage of the quantitative quality indicators and DESAP key assessment questions using scales like DESAP approach.

An example of these quality indicators is the following scale defined to CV for key variables: more than 50% is 1) unacceptable accuracy – between 20% and 50% is 2) little accurate – between 10% and 20% is 3) reasonably accurate – between 5% and 10% is 4) accurate – less than 5% is 5) very accurate. Other example is the Rate of completeness of metadata information. Each component of metadata information has the following weight:

Complete methodology of survey	40%
Summary methodology and Metadata in SDDS format	20%
Metadata in SDMX format	20%
Summary of Quality Report	10%
Quality Report (full version)	10%

Final percentage of completeness of these components is transformed to a 5 grade scale where 1 is less than 20%, 2 is more or equal than 20% and less than 40%, 3 is more or equal than 40% and less than 60%, 4 is more or equal than 60% and less than 80%, 5 is more or equal than 80%.

A Standard Quality Report was developed including detailed information about product and process quality and a table of quality indicators (Table 1) as summary. NSIs produce indicators to policy makers make decisions, so why don't NSIs elaborate indicators for internal decision making?

[6] DESAP – European self-assessment check-list for survey managers (Development of a Self-Assessment Programme)
[7] SWOT – Strengths Weaknesses Opportunities and Threats

Table 1: Quality Indicators

DIMENSION	INDICATOR	WEIGHT	VALUE (*)
Relevance	Information available on user satisfaction (DESAP: V/2) Overall relevance (DESAP: V/3) User satisfaction index (survey) Rate of available statistics	0.10 0.10 0.60 0.20	
	Relevance (Total)	**1**	
Accuracy	Over-coverage (DESAP: II/6) Under-coverage (DESAP: II/7) Misclassification (DESAP: II/8) Necessity of editing (DESAP: IV/4) Unit non-response (DESAP: V/15) Item non-response (DESAP: V/18) Appraise the coefficients of variation (DESAP: V/6) Coefficient of variation (estimated for key variables) Imputation rate	0.10 0.10 0.05 0.05 0.20 0.10 0.10 0.20 0.10	
	Accuracy (Total)	**1**	
Timeliness & Punctuality	Time lag between the reference period and the first publication of the preliminary or final results (DESAP: V/21) Punctuality of time schedule of effective publication (DESAP: V/22)	0.50 0.50	
	Timeliness & Punctuality (Total)	**1**	
Accessibility & Clarity	Rate of completeness of metadata information for released statistics Number of publications disseminated and/ or sold Number of accesses to Web Site / Databases	0.70 0.10 0.20	
	Accessibility & Clarity (Total)	**1**	
Comparability	Comparability across non-geographical domains (DESAP: V/24) Comparability over time (DESAP: V/25) Length of comparable time-series	0.25 0.25 0.50	
	Comparability (Total)	**1**	
Coherence	Coherence of results of different frequencies (DESAP: V/27) Coherence within same socio–economic area (DESAP: V/28)	0.50 0.50	
	Coherence (Total)	**1**	

(*) 1-No at all satisfactory; 2-No satisfactory; 3-Satisfactory; 4-Very satisfactory; 5-Extremely satisfactory

Quality Policy

Once quality indicators were defined, a set of quality objectives were established based on them. Quality objectives (Table 2) are like quality requirements established by internal and, in some cases, external users that NSI must comply.

Table 2: Matrix of quality policy deployment

SUBJECT	INDICATOR	MEASUREMENT	OBJECTIVES	ACTIONS TO BE TAKEN
User satisfaction	Satisfaction survey	Average of responses.	>= 4, before Aug-2009.	Make a Handbook and dictate seminars to explain users how to use the Index (CCI). Change the methodology and include more constructions typologies.
	Complains	No. solved complains / Total complains	>= 90%, before Aug-2009.	
Training	Training activities	Training hours / Total working hours	>= 5%, before Aug-2009.	Dictate introduction courses to new staff. Design new courses.
	Courses evaluation	No. Satisfied trainees / Total trainees	>=80%, before Aug-2009.	Conduct courses to trainers.
	Staff evaluation	Average of evaluations	>= 70%, before Aug-2009.	
Product & Process Quality	Relevance	Weighted Sum of Quality Indicators from Quality Report	>= 4, before Aug-2009.	Include more constructions typologies. Expand geographic scope.
	Accuracy		>= 4, before Aug-2009.	Upgrade the base period and products.
	Timeliness & Punctuality		>= 4, before Aug-2009.	Enhance processes in order to improve Timeliness and Punctuality.
	Accessibility & Clarity		>= 3, before Aug-2009.	Improve NSI's Web page to allow a better access to the CCI information.
	Comparability		>= 4, before Aug-2009.	Keep comparability with time-series when methodology will change.
	Coherence	No apply in the CCI pilot experience.		

NSI Quality Policy is a general quality framework defined by Top Management based on mission and vision of NSI, laws, codes of practice, codes of ethics and ISO standards. Furthermore, a matrix of quality policy deployment (Table 2) was established to explain how quality objectives will be reached. So the aim is to assure that quality indicators are monitored and the achievement of quality objectives is assessed.

Risk Analysis

An information security risk analysis methodology based on the international standard ISO 27005 (Information security risk management) has been adopted by the NSI to systematically use information to identify sources and to estimate risks (basis for risk evaluation, risk treatment and risk acceptance).

This methodology establishes steps to implement risk analysis and evaluation as follows:

1) **Identification and valuation of information assets** (papers, databases, software, hardware, services, people, reputation and image). Register an inventory of information assets with its corresponding owner. Confidentiality, integrity and availability have been defined as criteria to evaluate the impact and criticality that information assets have on processes and NSI (Table 3).

Table 3: Valuation of information assets

	Confidentiality	**Integrity**	**Availability**
Low	**Low**: information that is freely accessible by anyone, e.g., web site.	**Low**: the loss of integrity has no influence on the NSI's business.	**Low**: availability is not critical and is sufficient for the asset to be available within 48 hours.
Medium	**Medium**: the asset can be accessed by any member of the NSI without any restriction, but should not be accessible by external people.	**Medium**: the loss of integrity has a minor influence on the NSI's business.	**Medium**: asset available within a day and the unavailability of assets would cause a minor impact to the NSI's business.
Medium-High	**Medium-High**: only authorised staff. Unauthorised access would be noticed and should be avoided.	**Medium-High**: loss of integrity has significant influence on the NSI's business and should be avoided.	**Medium-High**: available within a few hours and the unavailability of assets would cause a significant impact on the NSI's business.
High	**High**: only specifically authorised staff. Unauthorised access would impact seriously on NSI and should be avoided in all circumstances.	**High**: loss of integrity has a very important negative influence on the NSI's business and should be avoided in all circumstances.	**High**: should be available all the time and the unavailability of assets would cause a very important negative impact on the NSI's business.

2) **Analysis of threats and vulnerabilities associated to each group of information assets**. It begins analysing a list of most common threats that might affect information assets. Then, the probability of threat occurrence is estimated (Table 4). Thereafter, the vulnerability level is calculated (Table 5), i.e., assesses the extent to which existing controls are sufficient or not to prevent or mitigate effects of identified threats. A combination of likelihood of threat occurrence and vulnerability level is used to determine the exposition degree of each threat with respect to information assets (Table 6). Finally, which aspects of assets (confidentiality, integrity and availability) are affected by threats is evaluated in order to estimate the impact of that threats have on information assets.

Table 4: Likelihood of threat occurrence

	Probability		
Frequency of use of assets	**High**	**Medium**	**Low**
Weekly or daily	Once a month or more	Between once a month and once a year	Less than once a year
Monthly, bimonthly, trimonthly	More than once a year	Between once a year and once every 3 years	Less than once every 3 years
Biannual, Annual or less	More than once every 2 years	Between once every 2 years and once every 5 years	Less than once every 5 years

Table 5: Vulnerability level

Definition	Scale
There are no controls or existing controls has been wrong implemented.	High Vulnerability
There are some controls and these are not adequate or sufficient to prevent the identified threat occur on the asset.	Medium Vulnerability
There are controls and these are adequate.	Low Vulnerability

Table 6: Exposition degree of each threat with respect to information assets

	Probability		
Vulnerability	**Low probability**	**Medium probability**	**High probability**
Low	Very low exposition risk	Low exposition risk	Medium exposition risk
Medium	Low exposition risk	Medium exposition risk	High exposition risk
High	Medium exposition risk	High exposition risk	Very high exposition risk

3) **Estimation of current risk level**. It arises from a combination of impact and exposition degree previously calculated (Table 7).

Table 7: Current risk level

	Exposition				
Impact	**Very low**	**Low**	**Medium**	**High**	**Very High**
Not Applicable	0	0	0	0	0
Low	1	2	3	4	5
Medium	2	3	4	5	6
Medium-High	3	4	5	6	7
High	4	5	6	7	8

4) **Maximum acceptable risk level**. Director General must define and document which risk level will be the maximum acceptable (see in Table 7, e.g., the maximum acceptable risk level is 5).

Table 8: Identified risks

Group	Threats	Probability	Vulnerability level	Exposition	Impact	Current Risk
Software	Unauthorized software installation or changes to the software	Low	Low	Very Low	High	4
Office equipments	Unauthorized access	Medium	Low	Low	High	5
Digital	Unauthorized dissemination or transmission	Low	Medium	Low	High	5
PC	Fire	Low	High	Medium	High	6
Printed	Unauthorized copy	Medium	Medium	Medium	High	6
People	Inappropriate behavior	High	Low	Medium	High	6

Group	Threats	Probability	Vulnerability level	Exposition	Impact	Current Risk
Image & prestige	Inability to meet users requests	Medium	Medium	Medium	High	6
Servers	Unauthorized access	Low	High	Medium	High	6
Databases	Breach of legal, regulatory or contractual requirements	Medium	High	High	High	7

Note: the information in this table is not true; it has been purposely altered to preserve the confidentiality of the original data.

5) **Risk treatment method**. Process of selection and implementation of measures to modify risk. The organisation must decide which option of risk treatment (implement controls to mitigate risks, risk assumption, risk avoidance, and risk transference) will be implemented.

6) **Risk treatment plan**. An action plan is defined to establish controls to be implemented in order to deal with risks. It means to identify, select and implement control objectives and controls. In other words, assign resources.

Table 9: Risk treatment plan

Group	Threats	Current Situation		Action Plan
		Controls	**Vulnerabilities**	**Controls**
PC	Fire	Backups stored outside the NSI's building.	• Smoke detectors are insufficient.	• Install smoke detectors in all critical areas.
Printed	Unauthorized copy		• Lack of control on printers or photocopy machines.	• Establish procedures to avoid left printed papers containing confidential information into printers.
People	Inappropriate behavior	• NSI has adopted & adapted the European Statistics Code of Practice and the ISI Declaration on Professional Ethics.	• Lack of dissemination among employees.	• Disseminate CoP and ISI Declaration on Professional Ethics.
Image & Prestige	Inability to meet users requests			• Improve estimations of resources needed to meet users' requirements.
Servers	Unauthorized access	• Physical access control to the server's room.	• Physical access control is broken • There is no technical assistance service to repair the physical access control.	• Repair the device. • Make a contract with an enterprise to get technical support to maintain the device.
Databases	Breach of legal, regulatory or contractual requirements	• Specific regulations establishing how to deliver databases. • Encrypted databases.		• Register all databases into the government agency responsible of this kind of registers.

Note: the information in this table is not true; it has been purposely altered to preserve the confidentiality of the original data.

7) **Residual risk**. The risk remaining after the implementation of new or enhanced controls is the residual risk. Director General should formally accept the residual risk.

Information Security Policies

The Information Security Management System Policy is a statement of overall intention and direction as formally expressed by the Director General of NSI, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (preservation of confidentiality, integrity and availability of information).

The ISMS Policy is the first document of the ISMS approved by the Director General and it has been disseminated among NSI's employees in order to assure that the general ideas of NSI's ISMS have been known by everyone. Other information security policies that have been approved are:

a) Information Security Risk Management Policy that refers to coordinated activities to direct and control an organisation with regard to information security risk (potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organisation).

b) Information Security Incident Management Policy defines processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents (single or a series of unwanted or unexpected information security events that have a significant probability of compromising organisational operations and threatening information security) [ISO 2005].

Documentation of the Quality & Information Security Management Systems

Excessive documentation required by ISO standards is a myth, since it is not necessary to document absolutely every process of the NSI. In fact, NSI itself should require its employees to prepare documents of each process with a detail level in accordance with activities to be done and who will execute them.

Survey Metadata are published based on standard SDDS [8] and SDMX [8] (ISO 17369) and DDI [8] standards are also used to document microdata information. A methodology document has been standardized to facilitate its use into all NSI surveys. This document has the same structure of ISO 20252 in order to assure that each element of the standard is taken into account. In accordance to ISO 9001, ISO 20252 and ISO 27001 requirements, following documents have been prepared: document control procedure, records control procedure, processes documentation, control of non-conformance procedure, corrective and preventive actions procedure, internal audits procedure, quality policy, quality manual, information security management system policy, information security risk management policy and information security incident management policy.

Processes analysis and quality improvement

A macro processes map was drawn to visualize all main processes and its interactions. In deep analysis were carried out supported by processes flow-charts. Also, a basic set of key process variables for quality improvement was selected. Process control charts were systematically used to notice critical points and determine if process is in statistical control or out of control. Only three key variables were charted: non-response, coding accuracy rate and editing rate, but we aim to study more variables as a standard procedure in the future. Process redesign was finally developed in order to improve its efficiency and effectiveness.

Integrated Quality & Information Security Management Systems

Records of the QMS are the evidence that activities have been done and its results have been recorded. They are a key component of any QMS and are used to analyse results with the intention of improve the QMS and also to assure QMS is able to be audited. Quality Indicators are a special type of QMS records that are very important to monitor supported by software tools.

Other key elements of the QMS are: process control based on documentation, software tools and control charts. Measuring user satisfaction (user satisfaction survey, user complaints, user feedback). Management reviews. Every year, Top Management must review the QMS to ensure that it remains suitable,

[8] SDDS – Special Data Dissemination Standard (FMI); SDMX – Statistical Data and Metadata Exchange; DDI – Data Documentation Initiative

adequate and effective. Opportunities to improve and the need to change the QMS, quality policy and quality objectives are assessed during the review. Assessments of quality objectives achievement must be done during management review phase and internal audits.

Continuous improvement is not only conducted by Managers, but by all staff through analysing information contained in the records of the QMS.

ISMS and QMS are completely integrated into the NSI's management system. Process oriented, Continuous improvement cycle (plan, do, check, act), Nonconformity management, corrective and preventive action plans, documentation management systems, internal audits and management reviews are tools and methods that both management systems have in common.

Internal Audits

Once a year internal audits are conducted by three statisticians from other Units trained in quality audits. They assess conformity with ISO 9001 and ISO 20252, but not only that. Auditors also evaluate responses of DESAP questionnaire and any other opportunities to improve product and process quality.

ISO 27001 audits will be conducted at the end of 2011. Internal information security auditors are being trained.

Certification

External Certification Audits do not assess if, for example, survey methodology (product design) is appropriate, but do assess if any exists and it was defined following a procedure. External audits evaluate, for instance, if quality objectives (product quality requirements) have been already reached or there are proper plans that lead to achieve those quality objectives in an established period of time. ISO 20252:2006 allows certificating a QMS (survey process quality) but not the product quality itself. Indirectly, it certificates the quality of statistical product by assessment of quality objectives achievement as it was mentioned before.

An important remark is that certifications would not be seen as an end in themselves, but as a means to guarantee that the QMS has been correctly implemented and as a learning tool.

Software tools

We have used free software tools that gave us support to the implementation process:

Microdata Management Toolkit is a microdata & metadata documentation tool from International Household Survey Network. eGroupWare (egroupware.org) is an open source software useful to manage non-conformity product and some others ISO 9001 and ISO 20252 requirements. e-Form (e-Form Solutions: www.eform.com.uy) is a powerful software that integrates all survey processes like questionnaire design, data capture tool, data processing, questions bank, metadata & microdata documentation, quality indicators management tool, quality reporting, process administration & documentation, QMS support to facilitate ISO 9001 and ISO 20252 certification. It is free for NSIs.

Meycor-KP is a good example of software that helps us to perform risk analysis of information assets. BPMS or work-flow software - like ProcessMaker or Apia - is truly useful not only to implement the quality management system (from designing the work-flow of each process until its execution), but also as information security incident management system.

Conclusions

It is strongly recommendable to start by a pilot experience in a small survey which allows the project to be managed easily. Then Top Management should define the action plan to be followed based on results gained from the pilot test. Extrapolating pilot project to the rest of NSI surveys has involved writing a handbook on how to implement ISO 20252:2006 in the NSI *[Segui, Federico 2009]*. It has already begun on March 2009 and the rest of NSI areas will be incorporated in the next two years. On the other hand, it has a con that can be easily solved when extrapolating to the whole NSI or if you decide to include other areas in

the certification scope. The disadvantage is that pilot survey must be treated like a complete organisation in order to comply with ISO 9001 and ISO 20252 requirements. Thus some support activities should be included as part of survey area duties like: training planning, employee profiles management, user satisfaction measurement and more, that generally concern to other NSI areas.

Towards certification in whole NSI at the first time may fail the project completely and disincline employees. It is very important that certification scope of that first survey covers all phases of survey productive process. In this way, it will be easily replicable into other NSI surveys.

We suggest implementing ISO 9001, ISO 20252 and ISO 27001 at the same time. ISO 20252 does not require an implementation or certification of QMS according to ISO 9001, but establishes as requirement implementing some kind of QMS into the organisation. Hence, implementing ISO 9001 is the best way to assure NSI has a QMS well implemented into the organisation. On the other hand, ISO 27001 is aligned with ISO 9001 so that they are complementary. They are focused on management systems. Both standards seek continuous improvement of the organisation's management systems through errors prevention actions whether related to quality or associated to information security (confidentiality, integrity and availability). Quality and information security are extremely related subjects into the NSI's management system. Besides information confidentiality, integrity and availability are key points of any management system. The organisation's efficiency could be affected if the information is not available at the place and time that it is necessary. This situation may cause to re-process some tasks wasting time and resources. The same scenario would be present if the information integrity is affected.

REFERENCES

Blyth, Bill (2006): Independent, Transparent, Externally Audited: The ISO Approach to Survey Process Quality Control. Paper presented at the European Conference on Quality in Survey Statistics (Q2006), Cardiff, United Kingdom, 24-26 April 2006.

Ehling, M. and Körner, T. (eds.)(2007): Handbook on Data Quality Assessment Methods and Tools. Eurostat.

Eurostat (2003a): DESAP – Development of a Self Assessment Programme, The European Self Assessment Checklist for Survey Managers.

Eurostat (2003b): Standard Quality Indicators. ESS Working Group "Assessment of quality in statistics", Luxembourg, 23-24 May 2005.

Eurostat (2009): ESS Handbook for Quality Reports. Methodologies and working papers, Eurostat.

ISO (2005): Information technology -- Security techniques -- Information security management systems -- Requirements (ISO/IEC 27001: 2005).

ISO (2006): Market, opinion and social research – Vocabulary and service requirements (ISO 20256:2006).

ISO (2008a): Quality management systems – Requirements (ISO 9001:2008).

ISO (2008b): Information technology -- Security techniques -- Information security risk management (ISO/IEC 27005:2008).

Segui, Federico (2009): Handbook on how to implement ISO 20252:2006 in the NSI.