M. Plata Andrés; A. Frutos Sicilia; C. Turmo Blanco, J. Muñoz-Guerra Revilla; A. F. Rodríguez Cano; C. Rodríguez Bueno

An Information Security Management System for the Doping Control Laboratory of Madrid: Achieving ISO 27001:2005 Standard

Laboratorio de Control de Dopaje, Consejo Superior de Deportes, Madrid (Spain)

Introduction

The kind of information managed in a Doping Control Laboratory is really of sensitive nature. The Doping Control Laboratory of Madrid is currently implementing a new information system. This information system will became the neural system of the laboratory, guiding technicians and capturing and saving all the information produced. Therefore, is crystal clear that the implementation of an Information Security Management System (ISMS) becomes a key point in the robustness of the whole system.

In order to understand what the ISMS means, it can be considered as the Quality System, but in terms of a safe management of the information. The goal of the system is to preserve the confidentiality (only allowed people can access to the information), integrity (prevent the changing of results) and availability, on which everything else depends. The implementation of the ISMS in a Laboratory allows warranting that the security risks are identified, managed and minimized according to a systematic and efficient way, such methodology leads to a continuous improvement in the information management.

Norm ISO 27001

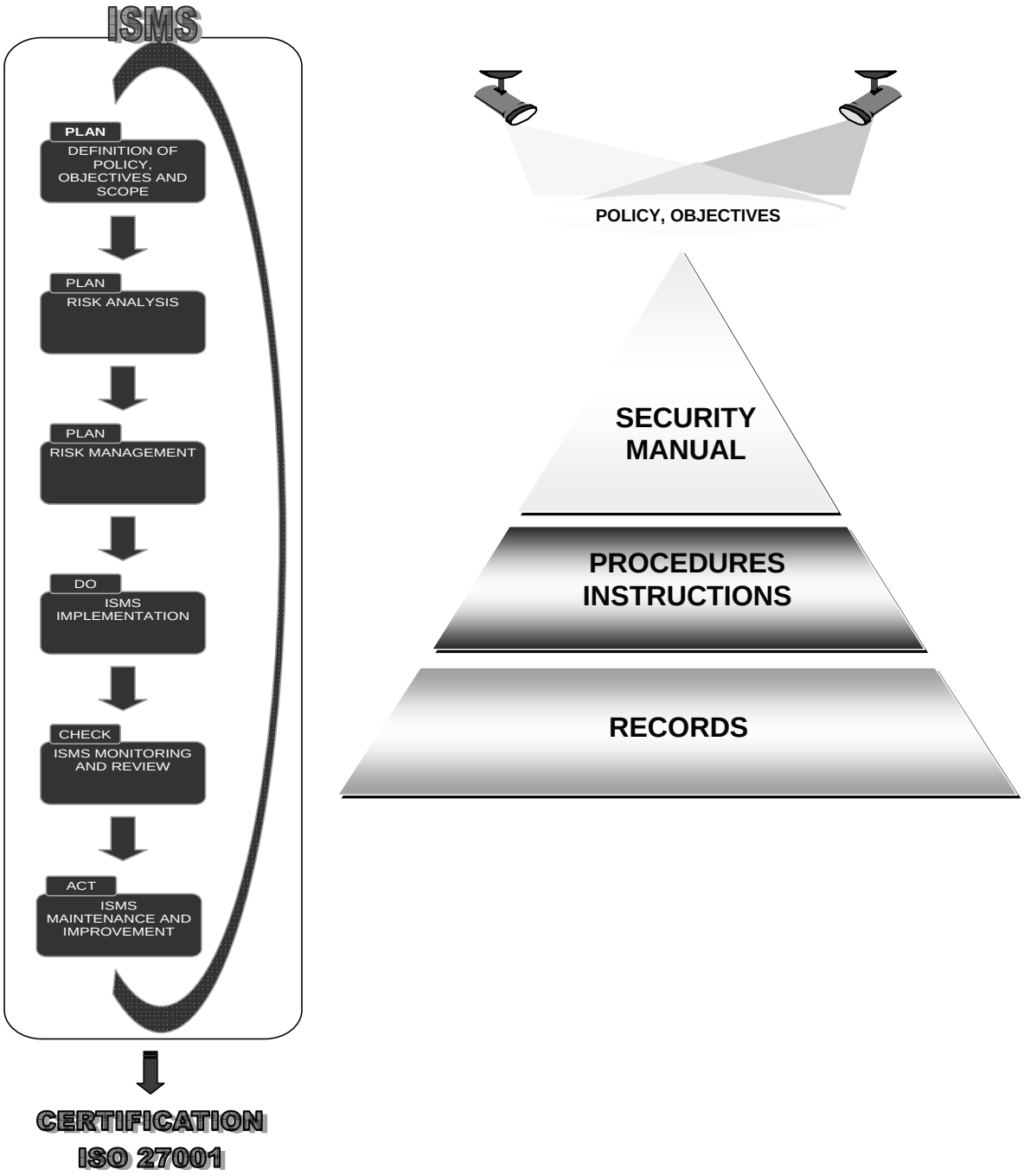
The Norm ISO 27001 is the workframe that makes possible to set up and implement in any organization an information security management system. The Norm is based in a cycle of continuous improvement (Plan-Do-Check-Act), similar to many others management systems (quality, environmental, occupational health and safety, etc).

The main activities for the implementation of norm ISO 27001 in a Doping Control Laboratory are:

1.- Definition of Security Policy

The Security Policy is a generic document where the management commitment and the focus of the organization in information security are described. It should be bearing in mind the legal and contractual requirements of the Laboratory in security terms. The

Security Manual will be comprised of the Security Policy along with the scope, the objectives, the description of the risk assessment methodology, the risk assessment report, the risk treatment plan and the Statement of Applicability.

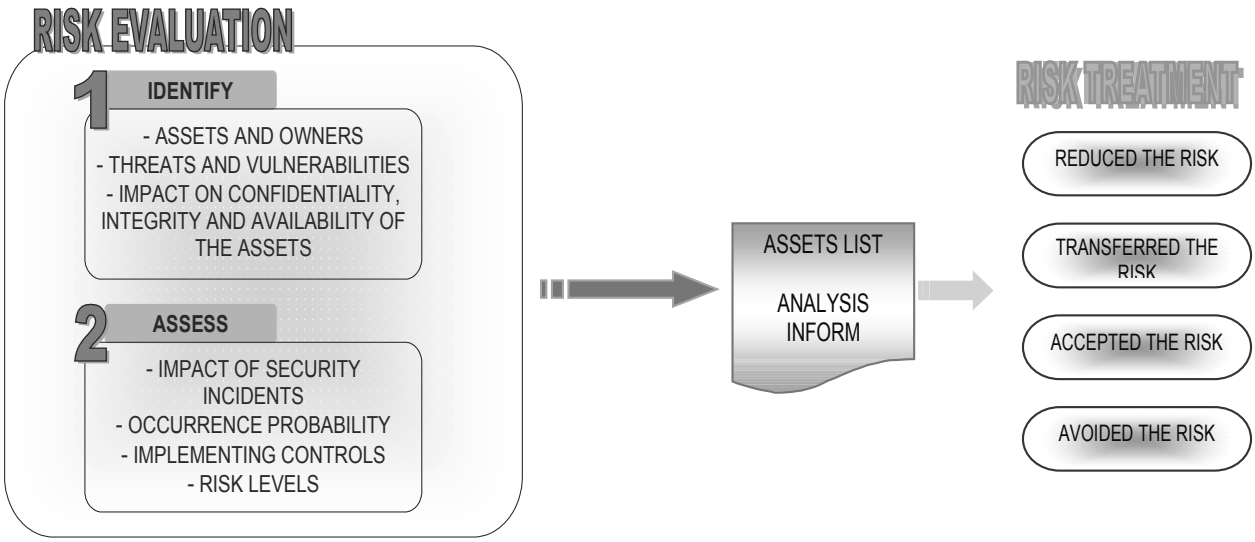


2.- Assets and owners

All the information assets should be identified and valued. An inventory should be done including the assets that have been considered important for the organization from a security point of view.

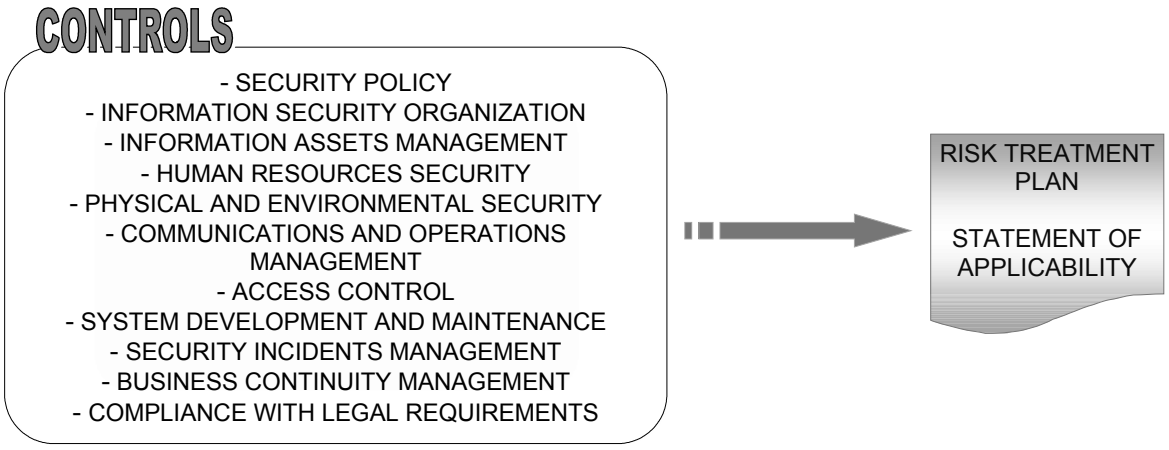
3.- Risk evaluation

It should be identified the threats or events that could have a harmful impact in the assets identified in the step before and the probability of occurring. The lost of confidentiality, integrity and/or availability of the assets should be taken into account during the evaluation of the impact of a security failure in the Laboratory.



4.- Selection and implementation of controls

Once they are identified, the controls that make possible to keep the risks to an acceptable level must be implemented. During the first steps of the system development, the information extracted from the first records makes possible to determine if the controls are really effective or should be modified, a new systematic evaluation and changes method allow to activate a cyclic and continuous way of improvement.



5.- Training

Laboratory personnel should be training and making aware about security of information. Asset owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained, and used.

6.- Review

The ISMS must be review on an on-going basis in order to guarantee the effectiveness of the system implemented.

7.- Certification

Once the system is implemented and working (3 months minimum) it can be certified by a third party.

Advantages of the implementation

For a Doping Control Laboratory the implementation of the Standard ISO 27001 can introduce advantages such:

- ✓ To decrease the risk of loosing, robbing or corruption the real sensitive information that is managed.
- ✓ To fulfil the security requirements established by WADA through the International Standards for Laboratories (ISL).
- ✓ The effective and secure management of the information can be demonstrated through the accreditation.
- ✓ The implementation of a continuous evaluation of risks and controls leads to identify the weak points of the system and allow to identify improvement areas,
- ✓ To reduce the costs with an improvement of the services.
- ✓ To establish a critical and systematic methodology of evaluation for the secure management of the information.
- ✓ As direct consequence, to increase the trust of the society in the antidoping system.

References

1. ISO/IEC 27001:2005. Information technology - Security techniques - Information security management systems – Requirements
2. ISO/IEC 17025:2005. General requirements for the competence of testing and calibration laboratories
3. El portal de ISO 27000 en español. http://www.iso27000.es/sgsi.html
4. The ISO 27000 Directory. http://www.27000.org/iso-27001.htm
5. Praxiom Research Group Limited**.** http://www.praxiom.com/index.htm#ISO%20IEC%2027001%20LIBRARY