SGSI project at CNAF

Andrea Chierici[1,*], *Donato* de Girolamo[1,], *Guido* Guizzunti[1,], *Stefano* Longo[1,], *Gaetano* Maron[1,], *Barbara* Martelli[1,**], *Cristina* Vistoli[1,], *Stefano* Zani[1,], *Gastone* Castellani[2,], and *Enrico* Giampieri[2,]

[1]INFN-CNAF, v.le B. Pichat 6/2 - 40127 Bologna, IT
[2]Physics and Astronomy Department, University of Bologna, v.le B. Pichat 6/2 - 40127 Bologna, IT

Abstract. The Italian Tier1 center is mainly focused on LHC and physics experiments in general. Recently we tried to widen our area of activity and established a collaboration with the University of Bologna to set-up an area inside our computing center for hosting experiments with high demands of security and privacy requirements on stored data. The first experiment we are going to host is Harmony, a project part of IMI's Big Data for Better Outcomes programme (IMI stands for Innovative Medicines Initiative). In order to be able to accept this kind of data we had to make a subset of our computing center compliant with the ISO 27001 regulation. In this article we will describe the SGSI project (Sistema Gestione Sicurezza Informazioni, Information Security Management System) with details of all the processes we have been through in order to become ISO 27001 compliant, with a particular focus on the separation of the project dedicated resources from all the others hosted in the center. We will also describe the software solutions adopted to allow this project to accept in the future any experiment or collaboration in need for this kind of security procedures.

1 Introduction

The adoption of an ISO-27001 certified ISMS [1] was triggered by the INFN participation to the international project HARMONY: "**H**ealthcare **A**lliance for **R**esourceful **M**edicines **O**ffensive against **N**eoplasms in hematolog**Y**" [2] under the Innovative Medicines Initiative 2 ("IM").

As information managed by the HARMONY project contain genomic data, it falls within the scope of GDPR (regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) [3], which defines a set of data protection rules for all entities operating in the EU, wherever they are based.

Article 4 of GDPR defines the role of Data Controller and Data Processor. A data controller is: "a natural or legal person [...] which [...] determines the purposes and means of processing of personal data". A Data processors "process personal data on behalf of the controller".

[*] e-mail: andrea.chierici@cnaf.infn.it
[**] e-mail: barbara.martelli@cnaf.infn.it

In the context of this project, HARMONY acts as Data Controller and appoints INFN-CNAF as Data Processor of the HARMONY Big Data Platform.

In order to be compliant to GDPR (art. 89), HARMONY, as Data Controller, must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with regulations. Such measures include the implementation of appropriate data protection policies by the controller. Adherence to approved certification mechanisms can be used as an element by which to demonstrate compliance with the obligations of the controller. For this reason, one of the HARMONY main requirements to INFN-CNAF is the achievement of the ISO/IEC 27001, well-respected and widely recognized international information security standard.

Beside the HARMONY collaboration, the capability to guarantee high-security standards can be an interesting opportunity for INFN-CNAF and future projects requiring strict security rules. Therefore, albeit the design and implementation of the present ISMS is influenced by needs, scope and objectives of the current project, it is expected to scale in accordance to the needs of the organization and future projects. The Big Data platform is capable of providing a scalable environment that allows to increase, on specific time peaks, computing and storage requirements in a single, secure and e efficient manner, taking into account that it will have to provide a multi-node hosting and high capacity storage environment.

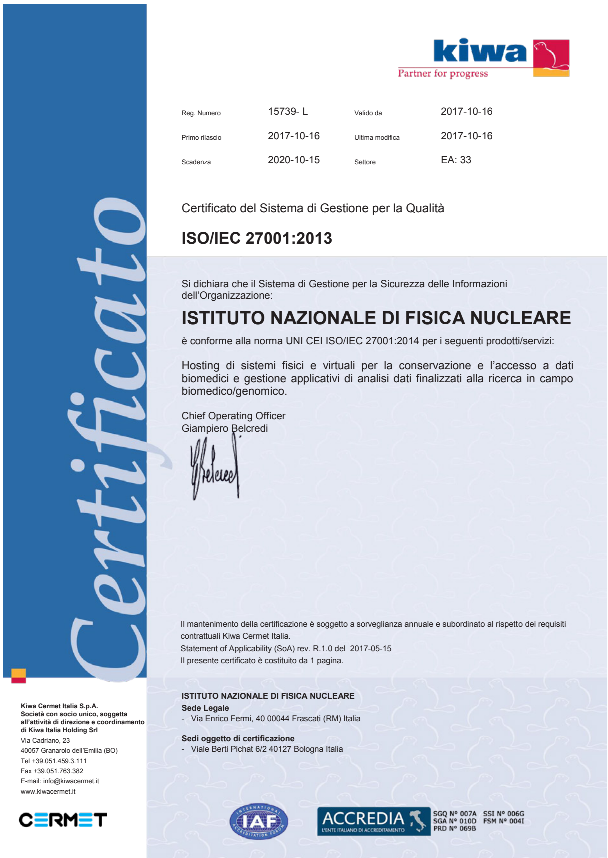
2 The ISO 27001 Standard

The ISO/IEC27000 family of standards helps organizations keep information assets secure, it focuses on management of information, not just IT/technical security. In particular ISO-27001 provides requirements for an **I**nformation **S**ecurity **M**anagement **S**ystem (ISMS or SGSI in Italian, both used within the paper).

An ISMS [4] is a systematic approach to manage sensitive company information so that it remains secure (in the sense of confidentiality, integrity and availability). It includes people, processes and IT systems by applying a **risk management process**. The design and implementation of an organization's ISMS is influenced by its business and security objectives, its security risks and control requirements, the processes employed and the size and structure of the organization. Therefore, maintaining an ISMS requires continuous adaptation to changing risks and systematic evolution trough a Plan-Do-Check-Act cycle (see Figure 1:

ACT
PLAN
DO
CHECK

Figure 1: PDCA for systematic improvements.



Certificato

kiwa
Partner for progress

Reg. Numero	15739- L	Valido da	2017-10-16
Primo rilascio	2017-10-16	Ultima modifica	2017-10-16
Scadenza	2020-10-15	Settore	EA: 33

Certificato del Sistema di Gestione per la Qualità

ISO/IEC 27001:2013

Si dichiara che il Sistema di Gestione per la Sicurezza delle Informazioni dell'Organizzazione:

ISTITUTO NAZIONALE DI FISICA NUCLEARE

è conforme alla norma UNI CEI ISO/IEC 27001:2014 per i seguenti prodotti/servizi:

Hosting di sistemi fisici e virtuali per la conservazione e l'accesso a dati biomedici e gestione applicativi di analisi dati finalizzati alla ricerca in campo biomedico/genomico.

Chief Operating Officer
Giampiero Belcredi

Il mantenimento della certificazione è soggetto a sorveglianza annuale e subordinato al rispetto dei requisiti contrattuali Kiwa Cermet Italia.
Statement of Applicability (SoA) rev. R.1.0 del 2017-05-15
Il presente certificato è costituito da 1 pagina.

ISTITUTO NAZIONALE DI FISICA NUCLEARE
Sede Legale
- Via Enrico Fermi, 40 00044 Frascati (RM) Italia

Sedi oggetto di certificazione
- Viale Berti Pichat 6/2 40127 Bologna Italia

Kiwa Cermet Italia S.p.A.
Società con socio unico, soggetta all'attività di direzione e coordinamento di Kiwa Italia Holding Srl
Via Cadriano, 23
40057 Granarolo dell'Emilia (BO)
Tel +39.051.459.3.111
Fax +39.051.763.382
E-mail: info@kiwacermet.it
www.kiwacermet.it

CERMET

IAF

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 007A SSI N° 006G
SGA N° 010D FSM N° 004I
PRD N° 069B

Figure 2: ISO 27001 certification.

- Plan: establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
- Do: implement and operate the ISMS policy, controls, processes and procedures.
- Check: assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
- Act: take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

3 ISO 27001 Implementation at INFN CNAF

In order to implement an ISO 27001 ISMS at CNAF, an extensive assessment and design activity has been carried out since 2016. After obtaining support by INFN-CNAF management and acquiring awareness that ISO 27001 implementation of an ISMS is a complex issue involving various activities, lots of people, and lasting several months, we chose to follow a project management approach in order to clearly define what is to be done, who is going to do it and in what time frame.

In a first phase we focused to complete the steps required for establishing a ISO 27001 compliant ISMS:

- define the scope and boundaries: we decided to implement ISO 27001 to a limited set of resources dedicated to the "Hosting of physical and virtual systems for biomedical data access and storage and for biomedical and genomic research application management"

- define the overall ISMS policy that should be approved by the management: it is the highest-level document in the ISMS, not very detailed, but defining some basic issues for information security in the scope of ISMS. The purpose is for management to define what to achieve, and how to control it. This was a very important step in order to guarantee that the management actively supports information security by giving clear direction (e.g. policies), demonstrating the organization's commitment and explicitly assigning information security responsibilities to suitable people.

- define the risk assessment approach of the INFN-CNAF: we chose a risk assessment methodology suited to the ISMS and we developed criteria for accepting risk. The point was to define the rules for identifying the assets, vulnerabilities, threats, impacts and likelihood, and to define the acceptable level of risk. The output of this activity was the definition of an Assets Inventory containing all important information about relevant assets like type of asset, format (i.e. software, physical, services, peoples, intangibles), locations, backup information, license information, and so on. This inventory has to be maintained and updated on regular basis during the whole ISMS lifetime.

In a second phase we:

- drew up a state of applicability (SoA) document listing the organization's information security control objectives and controls. The SOA is derived from the results of the risk assessment, where risk treatments have been selected, all relevant legal and regulatory requirements have been identified and contractual obligations are fully understood. Moreover, it summarizes a review of the organization's own business needs and requirements.

- drew up a risk treatment plan (RTP) identifying the appropriate management actions, resources, responsibilities and priorities for dealing with the information security risks identified in the risk assessment phase. This document is the core of the ISMS as it define the controls selection and implementation. It links to all four phases of the PDCA cycle.

- defined and implemented the ISMS program describing it in a set of documents (ISMS Manual, ISMS Procedures, ISMS Annexes) published in a reserved area of the INFN document management system. All documents are available to all and only the employees involved in the ISMS. During this step we tested the controls in order to verify if they met their respective objectives. We defined how to measure the effectiveness of controls and we started a security training programme for the staff involved in the ISMS.

- defined a ISMS review process which has to be performed at least once a year by the management in order to ensure the ISMS continuing suitability and effectiveness. The results of these reviews are clearly documented and maintained on the reserved area of the INFN document management system. This step is part of the "Check" phase of the PDCA cycle, therefore any corrective action arising must be managed accordingly.

In spring 2017 we were able to carry out a comprehensive review of the ISMS and SoA together with a certification auditor which demonstrated the compliance of the ISMS with the full PDCA cycle and with the continuous improvement requirement of the ISO 27001

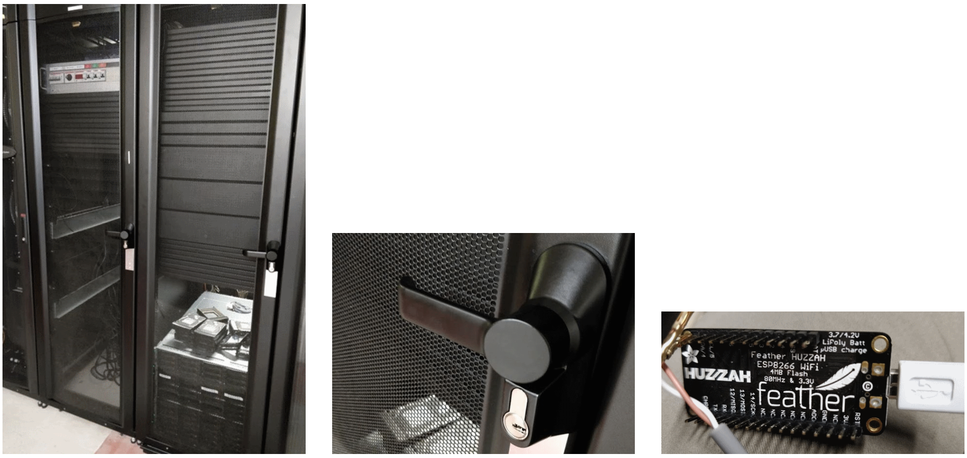


Figure 3: First ISO27001 deployment at INFN-T1.

certification. After few months of normal operations during which we settled down and tuned some procedures, we ran the official audit process that concluded successfully with the issue of the **ISO 27001:2014 certificate n. 15739- L**.

4 First deployment of an ISO27001 zone

The first implementation of an ISO 27001 zone was deployed during 2017, in a special area of the Tier1 "room 1". Some modification were necessary in order to enforce security, as requested by the protocol (see Figure 3):

- two racks were identified and dedicated to the project
- safe locks were installed, preventing unwanted access to machines hosted in the racks
- access control was enforced using rack door sensors (internally developed)

The SGSI requires isolation from most of the other, not secured, resources, and for this reason we had to duplicate most of the services already available. This services include:

- Bastion host: this node is the main front-end for external users wishing to log on computing resources hosted in the protected area

- IPA: an integrated security information management solution, used to manage credentials for the users in the secured area, completely separated from the ldap server adopted in the rest of the computing center

- Redmine: a project management web application, used for ticket management and for collecting documentation related to the project. Considering the fact that the node is not holding sensible data, it has been installed outside the secured area.

- Provisioning service: configured through a foreman server, holding all the software configurations of the machines residing in the secured area. Foreman uses puppet language to enforce the configuration across all the hosts.

- Log server: this node is critical for security reasons: it collects and stores all the logs coming from the machines in the ISMS zone. The admin password for this host is known only by a subset of the system administrator of the ISMS project. This is to enforce further security.

- Backup server: for security and redundancy reason this server is located outside the main computing room, holding encrypted data coming from all the nodes belonging to the various project hosted in the infrastructure. A further backup is performed on tape area network and soon will be duplicated in a remote INFN site (please remember all the data is stored encrypted)

This set of hosts and services is common for all the projects inside the ISMS zone. We allocated further hosts required by the harmony collaboration: currently 12 hosts are available to the project, configured following the project desiderata.

To access the resources from within CNAF network, a laptop has been configured specifically for the purpose. This laptop configuration enforces the highest security policies and users generally use it without admin privileges. Particular care was put on this host, that may be a weak point, if not properly configured: usb keys are not allowed, as well as generic web navigation and email access, that may allow malware inside the secured area. The use of this host has meant a change of mentality in CNAF sysadmins, and was not so well accepted in the first period, since it meant a more difficult access to resources.

5 Conclusions

The ISO 27001 certification was obtained for the subsystem dedicated to "Hosting of physical and virtual systems for biomedical data and for genomic research application management". This achievement is the result of an extensive effort involving a large part of the INFN-CNAF personnel and the Biophysics group of the University of Bologna. The certificate obtained is only the starting point of a continuous improvement process which requires a radical evolution of internal procedures and management policies. This certificate positions INFN-CNAF datacenter in good place for future collaborations which will require data security assurance and respect of quality standards. The first experiment to exploit this certification is harmony and in this paper we briefly described all the services that we installed and configured in order to allow the collaboration to work properly in a highly secured environment, enforcing all the requirements of a ISMS zone.

References

[1] Georg Disterer "ISO/IEC 27000, 27001 and 27002 for Information Security Management", Journal of Information Security, 2013, 4, 92-100.

[2] The HARMONY Alliance, https://www.harmony-alliance.eu/.

[3] GDPR regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

[4] Edward Humphreys, "Implementing the ISO/IEC 27001:2013 ISMS Standard", ISBN 1608079317, 9781608079315