SGSI project at CNAF

ISO-27001 Certification at INFN-CNAF

HARMONY

What is ISO/IEC 27001:2013 Certfication and why INFN-CNAF took it

INFN-CNAF Computing room hosts the INFN-Tier1 centre that is mainly focused on LHC and physics experiments in general.

Recently the area of activity has been widened thanks to a collaboration with the University of Bologna: an area inside the computing center was set-up for hosting experiments with high demands of security and privacy requirements on stored data.

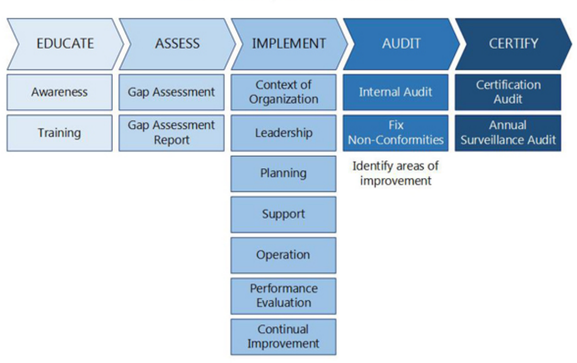
The first experiment that will be hosted in this area is Harmony, a project part of IMI's Big Data for Better Outcomes programme (IMI stands for Innovative Medicines Initiative). In order to be able to accept this kind of data, a subset of the computing centre had to be made compliant with the ISO 27001 regulation for a ISMS (Information Security Management System) dedicated to the "**Hosting of physical and virtual systems for biomedical data and for genomic research application management**".

ISO/IEC 27001:2013 is a specification for an information security management system (ISMS). Organizations that meet the standard may be certified compliant by an independent and accredited certification body on successful completion of a formal compliance audit.

Achieving accredited certification to ISO 27001 demonstrates that an institute/company is following information security best practice, and provides an independent, expert verification that information security is managed in line with international best practice and business objectives.

The ISO/IEC 27001 certification, like other ISO management system certifications, usually involves a three-stage external audit process defined by the ISO/IEC 17021 and ISO/IEC 27006 standards:
Stage 1 is a preliminary, informal review of the ISMS. This stage serves to familiarize the auditors with the organization and vice versa.
Stage 2 is a more detailed and formal compliance audit, independently testing the ISMS against the requirements specified in ISO/IEC 27001.
Ongoing involves follow-up reviews or audits to confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic re-assessment audits to confirm that the ISMS continues to operate as specified and intended. These should happen at least annually but are often conducted more frequently, particularly while the ISMS is still maturing.

ISO 27001 Implementation Process



INFN-CNAF ISO/IEC 27001 Implementation

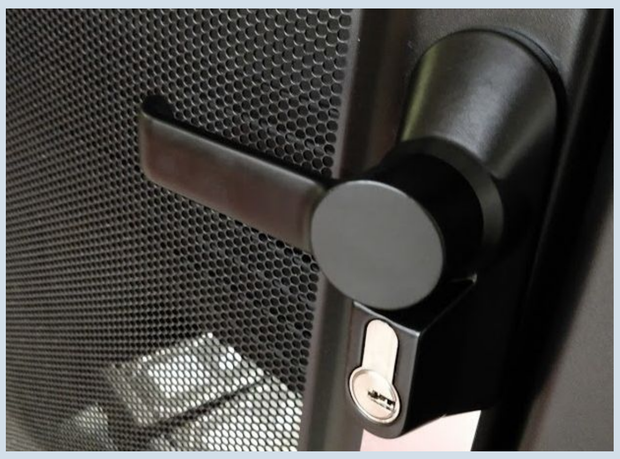
Complying with ISO27001:2013, has been a great effort for our center since we did not have strict procedures for physically separating hosts within the computing center.
To get the certification we had to:

- Install secure locks on rack doors
- Deploy door opening/closing sensors
- Logically separate the computing farm from the rest of the center
- Install core services targeted specifically to ISMS farm

Other important aspects:

- Access for external users is granted through a bastion host kept higly secured
- A separate ticketing system has been configured
- A centralized logging facility has been installed
- All the accounts are stored into an IPA server
- Monitoring system will be configured asap, through a separate server, publishing on general purpose CNAF dashboard.

Two racks with highly secure door locks



The computing farm

Door opening sensor, developed internally