# Harmonising ISO/IEC 27001 and ISO/IEC 17025 Implementation in the Digital Forensics Department, CyberSecurity Malaysia: A Case Study

*Ms. Sarah Khadijah Taylor, Mr. Mohd Zabri Adil B Talib*
*Digital Forensics Department, CyberSecurity Malaysia*

## Background

Aimed at providing quality and impartial service, the Digital Forensics Department (DFD) of CyberSecurity Malaysia (CSM) decided, in January 2007, to obtain accreditation from an accreditation body, American Society for Crime Lab Director/ Laboratory Accreditation Board (ASCLD/LAB) for its forensics services. The project was scheduled to be delivered in November 2011. The accreditation from ASCLD/LAB was based on the ISO/IEC 17025 *General Requirements for the Competence of Testing and Calibration Laboratories* and ASCLD/LAB's own Supplemental Requirements [1].

In the same year, CSM had successfully been certified with ISO/IEC 27001 Information Security Management System. The scope of the certification covered all departments under the CSM.

## ISO/IEC 27001 and ISO/IEC 17025

ISO/IEC 27001 is a standard that provides requirements for an information security management system (ISMS). ISMS is a systematic approach to managing sensitive company information so that it remains secure [2]. It includes people, processes and IT systems by applying a risk management process. It enables small, medium and large businesses in any sector to keep information assets secure. Being certified, CSM assures customers of data confidentiality, integrity and availability.

ISO/IEC 17025, on the other hand, specifies the general requirements for the competence to carry out tests and/ or calibrations, including sampling [3]. It covers testing and calibration performed using standard methods, non-standard methods, and laboratory-developed methods.

Chart 1 shows the requirements or clauses that both ISO standards have defined.


*Chart 1: Requirements defined in ISO/IEC 27001 and ISO/IEC 17025.*

## The Challenge

DFD had to conform to both ISO standards, ISO/IEC 27001 as well as ISO/IEC 17025, if they were to succeed in obtaining the accreditation. This was a challenge to DFD because it seemed like a far-fetched task. The questions that arose at that time were:

1. Can DFD create policies and procedures that are not conflicting with both ISO standards?
2. How many audits does DFD need to go through every year?
3. Will the decision to be accredited in ISO/IEC 17025 affect the current implementation of the ISO/IEC 27001 certification?

In this article, we will share with the readers the methods of harmonising the implementation of both standards.

## Harmonising ISO/IEC 27001 and ISO/IEC 17025

During the development of the policies and procedures in January 2008, DFD realised that some of the requirements, for example *Document Control* and *Physical Access Control*, were already in place and implemented by the organisation as a fulfilment to ISO/IEC 27001.

Although ISO/IEC 17025 required DFD to develop the same policies and procedures, the detailed requirements were not the same. For example:

a. ISO/IEC 17025 required management system documents to have end of page marking, whereas ISO/ IEC 27001 did not specify such a requirement.
b. ISO/IEC 17025 required that a list of approved vendors is maintained, whereas ISO/IEC 27001 did not specify such a requirement.

This posed a real challenge to DFD – could DFD harmonise both ISO standards without adversely affecting the whole organisation?

## The Mechanism

Several meetings and discussions were conducted in March 2008 between CSM's top management and DFD personnel to solve the matters. Thorough reviews of the requirements of ISO/ IEC 27001 and ISO/IEC 17025 were also conducted to look at similar areas. During the discussions, a level of understanding was reached and the methods for harmonising both standards were developed. Table 1 summarises the understanding and the methods implemented to ensure both standards would work hand in hand.

| No. | Matter | Action |
|---|---|---|
| 1 | **No Contradiction between both Standards**<br><br>Requirements specified in ISO/IEC 17025 and ISO27001 are not in any way contradicting each other. A standard may define more stringent requirements than the other, but never contradict it.<br><br>With this firm understanding, DFD can then move forward and start to develop its policies and procedures. | An understanding |
| 2 | **Supplement, not Supersede**<br><br>Should DFD need to add more clauses in the already implemented organisation's policies and procedures, DFD may specify the additional clauses in its own policies and procedures. However, reference to the organisation's policies and procedures must be made in the document.<br><br>For example, CSM has its own Organisation Document Control Procedure, adhered to by all departments. However the clauses in the procedure were not sufficient for ISO/IEC 17025. Thus DFD needs to develop its own Document Control Procedure. This procedure shall not supersede the Organisation Document Control Procedure; instead it will supplement it.<br><br>To implement this, DFD added the following clause in the opening of its Document Control Procedure: "*Organisation Document Control Procedure shall be adhered at all times. The DFD Document Control Procedure shall define additional clauses to fulfil ISO/IEC 17025 requirements.*" | Implementation |
| 3 | **Insert a saving clause**<br><br>Although both ISO standards do not contradict each other, there are some conflicts on the implementation level, between procedures outlined by CSM and those outlined by DFD.<br><br>For example, according to the Organisation Record Control Procedure, obsolete records shall be disposed in a central obsolete repository. However, since DFD owns classified records that cannot be distributed to internal staff, DFD has to manage its own obsolete records.<br><br>To implement this, DFD has developed its own Record Control Procedure. A saving clause was then added to the Organisation Record Control Procedure: "*Organisation Record Control Procedure shall be adhered at all times. Some department shall have its own implementation process, in which the department shall define the process in its own Record Control Procedure.*" | Implementation |
| 4 | **Audit some requirements once, but never twice**<br><br>DFD shall undergo internal audits twice annually, one for ISO/IEC 27001 certification and the other for ASCLD/LAB accreditation (ISO/IEC 17025). However, auditors for ISO/IEC 27001 certification shall not conduct audits on requirements that have been covered in the ISO/IEC 17025 audit and vice versa. This is done in order to reduce DFD workload. | Implementation |

*Table 1: An understanding of the standards that has been agreed by team members and the implementation methods of harmonising both.*

## Summary

The methods that have been put into practice in order to harmonise the implementation of both ISO standards have been successful. DFD has been working with both standards for almost four years without any glitches. The lesson learnt from this implementation is that team members must fully understand the requirements of both standards before making any decision so as to avoid redundant, complicated and lengthy implementation processes.

## References


1. ASCLD/LAB-International Testing Program. Available from: http://www.ascld-lab.org/international-testing-program/. [Accessed on 11th July 2014].
2. ISO/IEC 27001 - Information security management. Available from: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm. [Accessed on 1st July 2014].
3. ISO/IEC 17025:2005. Available from: http://www.iso.org/iso/catalogue_detail.htm?csnumber=39883, [Accessed on 2nd July 2014].