OIC-CERT Journal of Cyber Security
Volume 3, Issue 1 (April 2021)
1 - 6

Practical Guideline for Digital Forensics Laboratory Accreditation – A Case Study

Sarah Taylor, AkmalSuriani Mohamed Rakof, and Mohd Zabri Adil Talib
Digital Forensics Department, CyberSecurity Malaysia, Cyberjaya, Malaysia
sarah@cybersecurity.my

ARTICLE INFO

Article History
Received 04 Feb 2020
Received in revised form 07 Dec 2020
Accepted 08 Mar 2021

Keywords:
Digital forensics;
Digital forensics accreditation;
Forensic lab management

ABSTRACT

Digital forensics is a branch of forensic science that is used to assist investigation of cybercrime cases. Digital evidence, such as from mobile devices and computers, are analysed and the data are interpreted to assist the court of law in understanding what has taken place. In order to provide an assurance to the stakeholder on the accuracy of the forensic result, ISO/IEC 17025 has been used by forensic accreditation bodies to accredit laboratories. This paper, presents the case study in getting a digital forensics laboratory accreditation, the methodology, and the lesson learnt. This paper is hoped to provide guidance to those who would like to pursue accreditation for their Digital Forensics Laboratories (DFL).

I. INTRODUCTION

Digital forensics is defined as the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence. These evidences are derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations [1].

Digital forensics is used in investigation of crime cases. The digital evidence is analysed and the data are interpreted to assist the court of law in understanding what has taken place.

In order to provide an assurance to the stakeholders on the accuracy of the forensic results, a standard is applied to the work produced by a laboratory [2][3][4]. A notable standard for digital forensics laboratory (DFL) is the ISO/IEC 17025 [5].

This paper aims at presenting a case

ISSN 2636-9680
eISSN 2682-9266

study in obtaining accreditation for DFL. The work provides the following contributions:

- Methodology on getting accreditation.
- Lessons learnt in the journey of obtaining accreditation in order to increase the success rate.

II. BACKGROUND

A. Overview of the ISO/IEC 17025

The ISO/IEC 17025 *General Requirement for the Competence of Testing and Calibration Laboratories* specifies the requirements for a laboratory to perform its works [6]. This standard is applicable to all testing and calibration laboratories regardless of the number of personnel or the extent of the scope of testing and / or calibration activities.

Since this standard is meant for any laboratories, generally it is not sufficient for a DFL. Hence accreditation bodies, such as the ANSI National Accreditation Board (ANAB) from USA [7] and the Department of Standards Malaysia [8], produced supplemental requirements specifically for DFLs to fill in the gaps. This document adds critical requirement such as chain of custody and the requirement for the proficiency of analysts.

This ISO outlines 5 major requirements for DFL as follows:

i) General Requirement
ii) Structural Requirement
iii) Resource Requirement
iv) Process Requirement
v) Management System Requirement

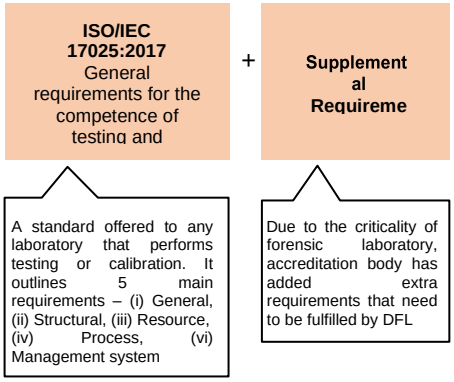

Fig. 1: Digital Forensics Laboratory (DFL) accreditation based on ISO/IEC 17025:2017 standard and accrediting body's supplemental requirement

The General Requirement addresses confidentiality and impartiality statements. The Structural Requirement, on the other hand, addresses the legality of the laboratory and overall responsibility of the lab and its organization. The Resource Requirement specifies the requirement for personnel, laboratory environment, equipment, and contractors. Meanwhile, the Process Requirement touches on request from stakeholder, methods, exhibits, reporting of results, complaints, nonconforming works, and control of data. The last requirement, the Management System, addresses risk management, corrective actions, internal audits, and management review.

B. Overview of accreditation

The ISO standard can be applied in DFL through self-regulation or accreditation [9]. Self-regulation depends on self-assessment and

attestation. Accreditation refers to the formal recognition by an independent body, known as the Accreditation Body, using technical experts that a DFL operates according to ISO/IEC 17025. ANAB [10] and the American Association for Laboratory Accreditation (A2LA) [11] from US, the National Association of Testing Authorities (NATA) [12] from Australia, and the United Kingdom Accreditation Service (UKAS) [13] from United Kingdom are examples of accreditation bodies.

In US, a consensus regarding accreditation has been reached through the summary of 13 recommendations made in the 2009 National Research Council report entitled *"Strengthening Forensic Science in the United States: A Path Forward"*. Among the recommendations are to mandate accreditation for all laboratories and facilities (public or private) and mandate individual certification of forensic science professionals [14], depicting the importance of obtaining an accreditation.

According to J. Kolowski [15], with accreditation, DFL is able to put a quality system in place and operational; demonstrating to stakeholders that the work is in good quality and provides a sense of assurance that work is done right.

Considering the erroneous convictions associate with the report from forensic scientist [16], which have caused lasting effects on people's lives, one might consider implementing a quality assurance in place to prevent such case from happening. The ISO 17025 accreditation, in general, does provide a minimal quality assurance for DFL.

C. Overview of Case Study

The Digital Forensics Department of CyberSecurity Malaysia has successfully obtained accreditation from the US accreditation body in 2011. The department has also successfully maintained its accreditation status until now.

Since the issuance of accreditation, it was observed that analysts were able to answer questions in court more confidently and less mistakes were made particularly human error such as grammatical erroneous in reports due to improper quality assurance in place.

In 2016, CyberSecurity Malaysia received a request from a middle east country to provide consultancy services in obtaining ISO/IEC 17025 accreditation. Not only have the agency successfully obtained the accreditation for the Client, but it has also successfully obtained it in just 14 months. The process of obtaining the accreditation will be explained in section III.

III. METHODOLOGY

The methodology that was used for obtaining the accreditation involves 8 major phases. Fig 2 shows the phases in a nutshell.

The first phase was conducting user requirement study. In this phase,

ISSN 2636-9680
eISSN 2682-9266

gaps between current practices and ISO requirements were identified and presented in a report. This process took 2 weeks.

The next phase was to develop the forensic process in writing. The documents that need to be developed were quality manuals, policies, procedures, technical procedures, and forms. Input from analysts were heavily sought in order to create an adaptable process flow. Creativity in developing a short process flow, and covers all essential forensic elements was crucial. The whole process took 8 weeks to complete.

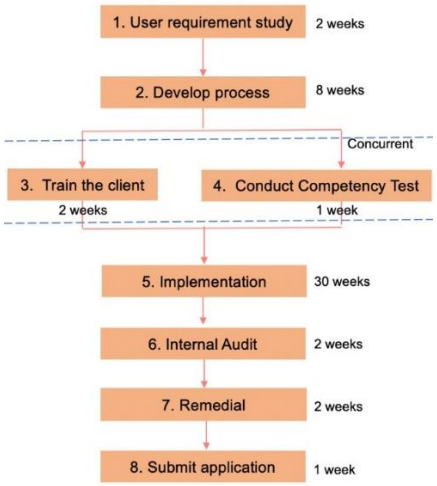

Fig. 2: Methodology of obtaining ISO/IEC 1702 accreditation

Once the forensic process has been laid out, next phase was a training session with the analysts. This process took 2 weeks and it was conducted concurrently with the Competency Test. It is a supplemental requirement from accrediting body that the organization must conduct a Competency Test for all its analysts to assess their competency level. Only when the analyst has passed the test can they be assigned with forensic cases. The test took a week. All the analysts of the Client's organization have passed the test.

With the process there and the analysts have been trained with the process, next was to implement the process. During this period, the Client must implement the forensic processes by themselves. Records must be created in order for the accrediting body to assess the implementation.

Phase 6 was the Client undergoing an internal audit. Three (3) auditors have been assigned to audit the Client's laboratory to ensure compliance with the ISO standard. The audit took 1 week, and the auditor took another week to produce the audit report. At the end of 2 weeks, the report was submitted to the Client.

Next, during Phase 7, the Client conducted the remedial phase based on the findings observed during the internal audit. In this phase, the laboratory must resolve issues raised by the auditors. Our Client thankfully did not encounter major issues, hence remedial works took a short period of time, which was only 2 weeks.

At the end of the process, an application for accreditation was submitted to the accrediting body. In order to assess DFL readiness, the lab needs to submit the written forensic process and internal audit report. Once they are satisfied with the developed documents, two (2) external auditors were sent by the accrediting body to observe implementation onsite. No major issues were observed by the auditors, and hence accreditation was

issued to our Client. This whole process took 2 months to settle. In overall, it took our Client 14 months to obtain accreditation from the first engagement with CyberSecurity Malaysia.

IV. DISCUSSION

Based on the observation of the whole accreditation process, it was found that it was doable to get accreditation in a short period of time, provided the lab is coached by experience personnel. The observations on other labs, particularly CyberSecurity Malaysia, on average it took between 3 to 5 years before a lab is awarded an accreditation. With the developed methodology, CyberSecurity Malaysia was able to shorten the duration to get the Client's lab accredited.

Second observation is that any labs that would like to pursue accreditation must undergo ISO 17025 training, including the senior management. This is important because without a good basic understanding of the ISO requirements, the implementation becomes difficult. For the analyst, when implementation was first introduced, they were having a hard time in understanding the extra work that they need to do. With basic ISO training, it will assist the management in explaining its importance and for analyst to understand the relevancy of the works.

Third observation was that in order for the internal and external auditors to audit the lab work, the lab must have real cases. These cases must be documented so that the auditors and assessors could evaluate the works.

The fourth observation was strong commitment and cooperation from the Client in order to keep up with the planned schedule. In this case, the Client had provided full commitment towards the plan and hence the success in obtaining accreditation in short period of time.

V. CONCLUSION

This paper presented a practical guide in obtaining ISO 17025 digital forensic lab accreditation. The methodology as well as the lessons learnt throughout the whole journey were listed. Future work would be to measure the effectiveness of having accreditation in a DFL.

VI. REFERENCES

[1] G. Palmer, "A Road Map for Digital Forensic Research," *First Digit. Forensic Res. Work.*, pp. 27–30, 2001.

[2] H. Guo and J. Hou, "Review of the accreditation of digital forensics in China," *Forensic Sci. Res.*, vol. 3, no. 3, pp. 194–201, 2018, doi: 10.1080/20961790.2018.1503526.

[3] A. M. Marshall and R. Paige, "Requirements in digital forensics method definition: Observations from a UK study," *Digit. Investig.*, vol. 27, pp. 23–29, 2018, doi: 10.1016/j.diin.2018.09.004.

[4] C. McCartney and E. Nsiah Amoako, "Accreditation of

ISSN 2636-9680
eISSN 2682-9266

forensic science service providers," *J. Forensic Leg. Med.*, vol. 65, no. April, pp. 143–145, 2019, doi: 10.1016/j.jflm.2019.04.004.

[5] E. H. Al Hanaei and A. Rashid, "DF-C2M2: A capability maturity model for digital forensics organisations," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2014-Janua, pp. 57–60, 2014, doi: 10.1109/SPW.2014.17.

[6] ISO/IEC 17025, "ISO/IEC 17025:2017 General Requirement for the Competence of Testing and Calibration Laboratories," *Int. Organ. Stand.*, vol. 2017, pp. 1–38, 2017.

[7] "Accreditation Requirements : ISO/IEC 17025:2017 Forensic Science Testing and Calibration Laboratories," 2019.

[8] "Specific Criteria 1.1 (SC 1.1) Specific Criteria for Accreditation of Forensic Science Testing," 2007.

[9] L. Wilson-Wilde, "The international development of forensic science standards. A review," *Forensic Sci. Int.*, vol. 288, pp.1–9, 2018, doi: 10.1016/j .forsciint.2018.04.009.

[10] "Forensic Accreditation." [Online]. Available: https://anab.ansi.org/forensic-accreditation. [Accessed: 04-Feb-2020].

[11] "Forensic Examination Accreditation Program." [Online]. Available: https://www.a2la.org/accreditation/forensics. [Accessed: 04-Feb-2020].

[12] "NATA accreditation in Forensic Science." [Online]. Available: https://www.nata.com.au/accreditation-information/accreditation-criteria-and- guidance/nata-accreditation-criteria-nac-packages/laboratory-accreditation-iso-iec-17025/category/20-legal. [Accessed: 04- Feb-2020].

[13] "Forensics." [Online]. Available: https://www.ukas.com/services/accreditati on-services/laboratory-accreditation- isoiec-17025/forensics/. [Accessed: 04- Feb-2020].

[14] J. M. Butler, "U.S. initiatives to strengthen forensic science & international standards in forensic DNA," *Forensic Sci. Int. Genet.*, vol. 18, no. January 2007, pp. 4–20, 2015, doi: 10.1016/j.fsigen.2015.06.008 .

[15] J. Kolowski, "The Challenge of Accreditation for Forensic Laboratories within the Good/Fast/Cheap Performance Management Paradigm," *Foresic Res. Criminol. Int. J.*, vol. 1, no. 1, pp. 2–3, 2015, doi: 10.15406/frcij.2015.01.0000 1.

[16] G. M. LaPorte, "Wrongful Convictions and DNA Exonerations: Understanding the Role of Forensic Science," *Natl. Inst. Justice J.*, no. 279, p. 16, 2018