United Kingdom Accreditation Service (UKAS) – Further supplementary written evidence (FRS0104)

Review of digital forensic laboratory applications for accreditation to ISO/IEC 17025 from July 2015 to August 2018

Background
As the National Accreditation Body for the UK, UKAS has been accrediting forensic organisations against the requirements of ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories and its predecessor NAMAS M10 since the late 1980s. The early accreditations covered the traditional scientific disciplines such as body fluids, drugs, toxicology and forensic chemistry. Over the decades forensic organisations have requested further extensions to their accredited scope to cover a wider range of disciplines. From about 2000, UKAS received its first applications for digital forensic activities and between 2000 and 2004 it awarded accreditation in the areas of computer, mobile phone, video and audio examinations. This accreditation was against the requirements of ISO/IEC 17025.

Only a limited number of forensic organisations held and maintained accreditation for digital forensic activities prior to the then Forensic Science Regulator (FSR), Andy Rennison, announcing in December 2011, through the Statement of Requirements, that all digital forensic activities were to be covered by ISO/IEC 17025 accreditation by 2015. The specific requirements and deadlines for digital forensics as listed in the Statement of Requirements have changed since the initial announcement in 2011, and it is UKAS’ understanding that this has been as a result of feedback from the digital forensic community regarding their readiness and ability to meet the original 2015 deadline. A new deadline of 2017 for the majority of digital forensic disciplines was set in August 2014.

Since the setting of the Oct 2017 deadline UKAS has helped organisations prepare for their assessment, and to gain an understanding of the UKAS processes and assessment approach. This assistance has been in the form of two workshops held in 2015 and 2016 for the digital community (funded and facilitated by the FSR). During the period 2015 – 2017 UKAS ran approximately ten ISO/IEC 17025 Forensic Laboratory Management training courses, with a number focused specifically on digital forensics.

Following the first visits to police digital forensic units, UKAS provided feedback directly to the police Quality Managers and digital representatives on the type of issues being identified and the actions that they could take to increase their state of readiness. UKAS has also contributed to digital forensic accreditation awareness workshops run by the Charter Society of Forensic Sciences, and to regular engagement with the National Police Chiefs’ Council Digital Forensic Portfolio board to assist and provide feedback on the digital forensic communities plans for accreditation.
UKAS currently undertakes the accreditation of digital forensic activities against the requirements of ISO/IEC 17025, along with the specific forensic guidance documented in ILAC-G19:08/2014 *Modules in the Forensic Science Process* and also to the FSR Codes of Practice and associated digital appendices (for organisations that are already accredited to the Codes or have requested assessment against them). The content of this report mainly relates to the issues highlighted during the assessments to ISO/IEC 17025 and ILAC G19.

**Summary of the current situation (as of 31st August 2018)**

- There are currently 30 legal entities which hold accreditation for one or more digital forensic activities at one or more locations.
- The 30 accreditations cover 6 private companies, 3 government organisations and 21 police forces. A number of the police forces which hold the accreditation additionally take responsibility for work undertaken at digital forensic units situated within other force areas under a collaborative agreement.
- Of the 30 entities the scopes of accreditations include 28 “Imaging of Computer Media”, 8 “Analysis of computer media”, 16 “mobile phone examinations”, 2 “Sat Nav examinations”, and 3 “CCTV”. To date no accreditations are held for “audio”.
- There are currently 52 Extension to Scope/Initial Assessment applications in progress with the two oldest applications being received in July 2015. (11 were received in 2016, 25 in 2017 and 14 in 2018). Where these are on hold this is at the request of the organisation due to their lack of readiness.
- From the initial application through the process of assessment to the grant of accreditation, the scopes of many of the accreditations were reduced (activities and locations) due to the readiness of the organisation and / or lack of compliance witnessed during the assessment visits.
- UKAS has suspended digital forensic activities at 2 organisations, these accreditations have been subsequently re-instated following extra visits to confirm compliance.

**Key issues identified during the first digital forensic assessments**

From 2015 to the end of August 2018, UKAS undertook approximately 61 initial assessments or first extensions to scope of forensic units for the different digital disciplines (e.g. computer, phones, video). Further extension to scope assessments (e.g. extending number of tools or sites) have been undertaken, however, the statistics in this report only relate to the first assessment of a forensic unit for that specific discipline.

The findings raised during these assessments have been reviewed to provide the data for this report. In addition, feedback from UKAS Technical Assessors has also been included on the general trends identified on visits. During these 61 assessments, 3,083 findings were raised in relation to adherence to ISO/IEC 17025 and ILAC G19 requirements with 2,972 being mandatory findings (a non-conformity requiring action to be taken to become compliant) and 111
recommended findings (suggested improvement action). A breakdown of average numbers of mandatory findings per discipline is provided in Table 1.

<table>
<thead>
<tr>
<th>Digital Forensic Discipline (No of assessments)</th>
<th>Average number of mandatory findings per visit</th>
<th>No. of assessments resulting in no offer or a restricted scope.</th>
<th>% of assessment requiring extra visit</th>
<th>Average length from application to grant (months)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer (36) (Imaging and analysis combined)</td>
<td>50</td>
<td>7</td>
<td>53</td>
<td>20</td>
</tr>
<tr>
<td>Phones (20)</td>
<td>47</td>
<td>7</td>
<td>55</td>
<td>14</td>
</tr>
<tr>
<td>Video/CCTV) (5)</td>
<td>44</td>
<td>0</td>
<td>100</td>
<td>21</td>
</tr>
<tr>
<td>Overall</td>
<td>49</td>
<td>14</td>
<td>56</td>
<td>19</td>
</tr>
</tbody>
</table>

Table 1 – Outcome of digital assessments

Table 1 also shows the number of assessments which did not resulted in a positive recommendation for grant of accreditation or could only make a positive recommendation of accreditation for a reduced scope, the average number of assessments which required an additional assessment visit and the overall period of time from application to grant of accreditation.

From reviewing the breakdown of the ‘findings’ it was established that the three main areas of non-compliance were in the implementation and maintenance of a management system; the lack of technical procedures or detail within the complete technical process; and the provision of data to support the validity of the methods. However, the number of findings in specific areas does not necessarily highlight the technical significance of some of the non-conformities. A summary of some of the main issues identified through the review of findings raised at assessment and also feedback from the Technical Assessors are provided below under the relevant heading along with a few examples of findings raised during the 61 assessments (this information has been anonymised and provided in Italics).

**Technical Procedures**
This area was found to be a major weakness in all digital forensic disciplines, whereby there were a lack of procedures covering the whole technical process and where procedures existed they contained insufficient detail to ensure consistent application or effective direction to staff on what should be undertaken on a routine basis. The Technical Assessors found it difficult to determine what was the organisation expected process when variation between forensic staff was observed during an assessment.
“SOP-X does not describe in sufficient detail the procedures to follow to cover all stages of the extraction and examination process e.g. guidance on how to handle exhibit, order of examination, which tools to use, what equipment to use, what settings should be used for Imager, how to verify output.”

**Technical Practice**
Technical Assessors commented that there was often variation in practices being employed within the same digital forensic units. The main findings raised related to staff not following the unit’s documented procedures; others related to good practices which were not being shared with others in the unit and on a few occasions poor practices were witnessed. While this was not one of the areas where a large number of findings were raised they do highlight inconsistent practice within units and lack of previous standardised approaches. Examples of some of the more significant findings in this area are provided below:

“The two locations under this application adopt a different approach to verification of the data extracted from mobile devices.”

“An inappropriate functionality test of a laptop was performed after imaging which could have made changes to the evidential media. The performance of this test (or otherwise) and other elements of re-assembling devices was not covered in the Standard Operating Procedure (SOP).”

**Technical Records**
The assessments highlighted an area of weakness in the technical records being made and retained by a number of digital forensic units. Instances of poor photography were witnessed along with a lack of detail in associated notes such that work could be repeated, or critical decisions and findings identified.

Other records related issues were around the traceability of electronic notes to the individual making them, as well as the ability to identify any (un)intentional changes. A number of issues have been identified with the back-up processes for electronic information and security of IT equipment.

“The notes produced for the witnessed activities would not enable another expert to identify any critical issues with the process and identify any trends at a later date. It would further not allow for another expert to examine if an appropriate course of action had been followed during the examination.”

“Imaging notes are recorded contemporaneously but are not protected in a manner which prevents alteration. They are created and held in a digital format within a word document. This is available in a mutable format within shared directory structure for the case. Changes are not identifiable at the time of creation of notes.”

**Training / Competency**
The assessment teams were often able to confirm that the digital forensic staff had the necessary competencies through the witnessed activities on the
assessments. However, there was generally a lack of detailed training procedures within the digital units to ensure that new staff or personnel recruited with previous experience will undergo a defined training process. In addition, a common finding raised on assessments relates to the digital forensic units not having objective evidence to demonstrate the competency of their staff other than relying on staff attending courses and having previous years of experience. Another common finding relates to digital forensic units not having a mechanism to demonstrate on-going competence once individuals had been initially signed off.

While findings were not always raised (due to the fact the digital forensic units were managing the competency issues identified), the assessment team reported that a number of units had identified competence issues with staff after they had implemented the ongoing competence evaluation process.

"The current requirements for evidence of training and competency consists of one test, this is not sufficient to demonstrate competence given the number of variables that can be encountered”

"Staff have been authorised as competent to perform tasks in the digital forensic unit; however, the manager that has conducted this evaluation is not technically competent to do this.”

**Validation**

The issues with validation were common across the different digital forensic units and related to the fact that the initial validation focused on tool verification and not overall method validation. In addition, the tests undertaken did not cover the significant risks in the process or appropriately stress test the method (appropriate test data or devices); there was no identification of the main uncertainties in the method and the lack of evidence to demonstrate that the method is repeatable within the organisation. Often the validation exercises undertaken did not follow the structure detailed in the FSR Code of Practice and staff were often unaware of the FSR Digital Validation appendix.

A number of the forensic units identified issues with the method or tools as part of their validation exercises. However, the outcome of the validation was not always communicated to the digital forensic staff nor the relevant procedures updated to ensure appropriate actions would be taken as a result of the validation. Finally, as validation is a relatively new concept to the digital community there was no mechanism in place to deal with changes in the methods (in particular updates to forensic tools) in relation to demonstrating the on-going suitability of the method.

"To date no validation has been completed for any method in the proposed scope.”
“The results of Method Validation work have not been communicated to staff engaged in the forensic processes in scope, therefore they are not aware of the details of success and or limitations.”

“The mobile phone examiners are not aware of whose responsibility it is to validate hardware and software. Also they do not know if the equipment and software that they are using has been validated.”

“Assessments of whether software updates would, or would not, trigger further validation are inadequate and not implemented”

**On-going Quality Assurance**

The assessments identified that the digital forensic units had often not implemented a robust on-going quality assurance mechanism at the time of the assessment visits. Some staff in organisations were undertaking informal dip checking of their own work but there was no structure and consistency amongst staff. Secondly, there was a level of periodic independent checks on work which only involved a paper review of records against the submitting customers request. None of the existing quality checks involved a robust assessment of the technical validity of the work and would provide assurance that any significant amount of data had not been missed or that tools had been used appropriately.

A common finding raised related to lack of awareness of Proficiency Testing (PT) schemes and active participation in any other external quality assurance activities e.g. (Inter Laboratory Comparison (ILC)). In a number of instances PT/ILC expectations had not been met, however, the organisation had not undertaken an appropriate investigation to identify the reasons for the errors.

“A review of records in the case management system and casefiles showed, that for a significant number of 2017 cases, no case strategy, no quality check, no dip sample had been performed.”

“The quality assurance mechanisms at present do not provide on-going assurance on the reliability of work being delivered out of the unit. The QA process on each case provides assurance that notes are appropriate but there is nothing in place to provide assurance that data has not been missed or the technical work has been undertaken appropriately.”

“For the ILC imaging trial undertaken in 2016, differences in outcome achieved by the two sites have yet to be the subject of effective investigation and formally recorded within the QMS.”

**Reporting of Results**

The assessment team witnessed a wide range of ways the results of the examinations are provided to the customers of the applicant organisations. Some of the outputs have involved the customer receiving multiple extractions of data generated via different examination tools, yet containing similar but not identical information, and requiring them to determine which is the best one to
use. It was found that digital forensic units rarely produce statements or are required to attend court. In many instances staff have not received appropriate court awareness training and / or did not have access to template statements if a request was received. In addition, knowledge of the criminal procedure rules was mixed.

In a couple of digital forensic units, it was found that staff in training were undertaking live casework and taking responsibility for the work, and producing associated statements, prior to completion of their training and any official sign off relating to their competencies.

"Statements are being issued by staff that are not signed off as competent to complete the work. There is no reference in the statements and contemporaneous notes that the staff member is not signed off or reference to who has taken responsibility for the work completed e.g. the mentor is not referenced."

Exhibit Handling
Exhibit handling in the main was appropriate, however, it was common to find poor records relating to the chain of custody for an exhibit and also that digital units often accepted poorly packaged and labelled exhibits. This was a more significant issue in the video/CCTV related area.

"The Digital unit does not have control over the integrity/continuity of an exhibit when it is left unattended during the acquisition process."

"The current systems in place do not show a clear chain of custody of item movement within the department."

Other Relevant Findings
The previous sections of this report highlight the more common themes in the findings that have been raised during digital forensic assessment. However, the majority of assessments have raised findings against all sections of ISO/IEC 17025. Some other significant issues identified were as follows:

"Of the 8 non-conformances raised in 2017, arising from audit, only 2 have been closed in reasonable time scales, 4 have taken 5-6 months to close and 2 remain open".

"The audits which were reviewed had not highlighted a level of non-compliance commensurate with that found during the UKAS assessment. It is therefore unclear as to whether the appropriate breadth and depth of reviewing of the processes associated with this Extension To Scope (ETS) have been included in audits."

"At present there are over 200 mobile phone submissions held awaiting analysis within the Forensic Submissions unit and past SLA TRT’s".
“The storage facilities currently used for historic records are unsuitable as the files/records are deteriorating and there is insufficient space. The storage order does not facilitate easy retrieval.”

Summary and General Conclusions
Between 2000 and 2015, UKAS had accredited a small number of organisations against ISO/IEC 17025 and ILAC G19 for digital forensic disciplines including computer, phone and video examination. Since 2015 approximately 30 organisations with 57 separate digital disciplines (see Summary on page 2) have been accredited. Therefore, the level of accreditation obtained in the digital forensic community to date demonstrates that ISO/IEC 17025 is achievable in all the main activities.

From UKAS’ involvement in accreditation workshops, digital forensic working groups and the general accreditation process it is clear that the digital forensic community is struggling to grasp the concepts of accreditation and how they can evidence compliance against the core requirements of ISO/IEC 17025 (e.g. implementing an effective quality management system along with having objective evidence demonstrating staff competency, validity of method and assurance on the reliability of output). This is reflected in the number of mandatory findings, on average 49, being raised on the first assessment of a different discipline within a digital forensic unit, and therefore demonstrating the value of assessments in identifying improvements through the accreditation process.

The witnessing of digital forensic activities during the assessments has provide a level of assurance of the competence and knowledge of staff undertaking the examinations. It has also identified a number of good practices which may or may not be part of the technical procedures. However, from the first assessments there is limited objective evidence to provide assurance that the organisation can, and is, producing reliable results. The main evidence which digital forensic units have provided at the early stages is that their staff are competent (mainly via attending training course and years of service) and that they use commercially available forensic tools for which supporting data of validity is not available. There has been limited objective evidence which provides assurance that the units are producing reliable outputs until the digital forensic units have introduced the main requirements of ISO/IEC 17025 (e.g. validation of methods, competency assessment of staff, quality assurance protocols). It is therefore evident that without accreditation digital forensic units would not have sufficient appropriate objective evidence to support the reliability of their output.

With the currently level of knowledge and competence in accreditation within the digital forensic community it is taking on average 19 months from the time that an application is received by UKAS until an organisation gains accreditation. It has been shown to be possible to gain accreditation in 9 months but has taken as long as 26 months. With the level of non-compliance witnessed at the first assessment there has been a requirement to undertake extra assessment visits.
in 56% of cases which introduces additional accreditation costs. The level of findings being raised also has had an effect on these costs due to extra office time required to review the close out evidence. The average number of findings raised at an assessment visit has been 49 with as few as 11 and as many as 136. So, two scopes of similar size were compared with a variance of approximately 10 days (~£8.7K). **Therefore, it can be seen that the readiness of the organisations has a direct impact on the cost of their accreditation.**

Although this report has been focused on the first assessments of digital forensic units for specific disciplines it has been seen that compliance has generally improved in subsequent surveillance visits with many digital forensic units now refining and implementing effective quality assurance and validation procedures. However, conversely, a few organisations have struggled to maintain the impetus of the initial accreditation which has resulted in extra visits in the surveillance cycle to ensure effective implementation and in a couple of instances this has been of such significance that it has resulted in suspension of accreditation.

**Overall, this report demonstrates that digital forensic activities can be accredited and that the international standard ISO/IEC 17025, together with ILAC G19 and the FSR’s Code of Practice, provides a suitable mechanism for the community to demonstrate, via objective evidence, the reliability of the methods (procedures, equipment, staff) they use and the output they provide to the Criminal Justice System.**

4 January 2019