UK ISO 17025 Digital Forensics Survey April 2017: Results

Over the last 12 months we have become aware of growing concern among practitioners in digital forensics about the impact of planned regulation of forensic science services in general. The concerns have been around the appropriateness of the chosen standard – ISO 17025 – and the costs of implementing it.

The stated aim of the Forensic Science Regulator is to require those serving the Criminal Justice System to be compliant, at least for a first stage of evidence preservation via forensic disk imaging, by October 2017.

A small group of experienced practitioners, including those who have trained many others and have previously advised the Forensic Science Regulator decided it would be useful to gather firm evidence of these concerns and to test them. Plainly it would not be enough simply to ask for complaints. We, and policy makers, need to know something of the shape of the existing industry that supplies digital forensics services. Which services are being offered? Are they coming from large organisations, medium-sized ones, or sole traders? What levels of training have practitioners undergone? What standard operating procedures or good practice guides do they follow? How far are they compliant with various external standards? What is impact of the existing Criminal Procedure Rules on expert evidence? Which analysis tools do they use, and how far have these been tested / validated / verified? What is the level of existing knowledge about ISO 17025? For those that have gone for ISO 17025 what have been the associated costs? What has been the cost impact of ISO 17025 compliance?

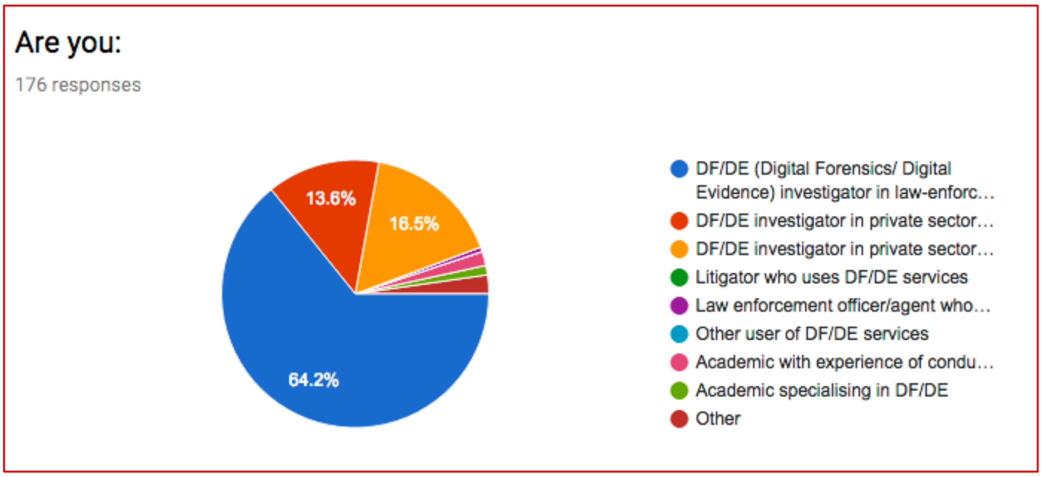
These and other questions were converted into a survey format and use made of the Google Forms facility. The survey was aimed at individuals who work in digital forensics, as opposed to organisations. Options were provided for informal text-based responses as well as straight choices.

There is no single reliable list of all who offer digital forensics services to the UK criminal justice system. In order to attract responses publicity was generated via F3 – the First Forensic Forum - and the online magazine Forensic Focus. It was hoped that knowledge of the survey would ripple out.

In the end 180 responses were received. Given the circumstances and that respondents made a specific choice to complete the survey form we cannot claim that the results are "representative". Nevertheless we believe that the quantity of responses is more than sufficient to influence the development of policy in relation to maintaining and increasing the quality of digital forensics services to the criminal justice system.

As this survey has been carried out on a part-time basis and with no funding this print report has been assembled by cutting and patching from the electronic data produced by Google Forms.

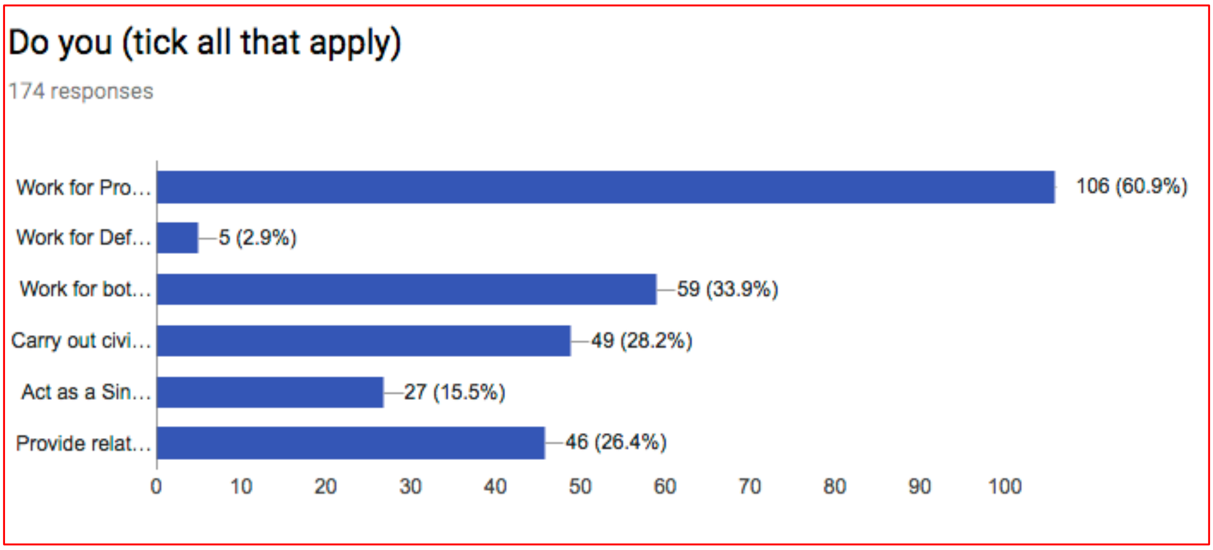
Pat Beardmore, Geoff Fellows, Peter Sommer and others



Are you:

176 responses

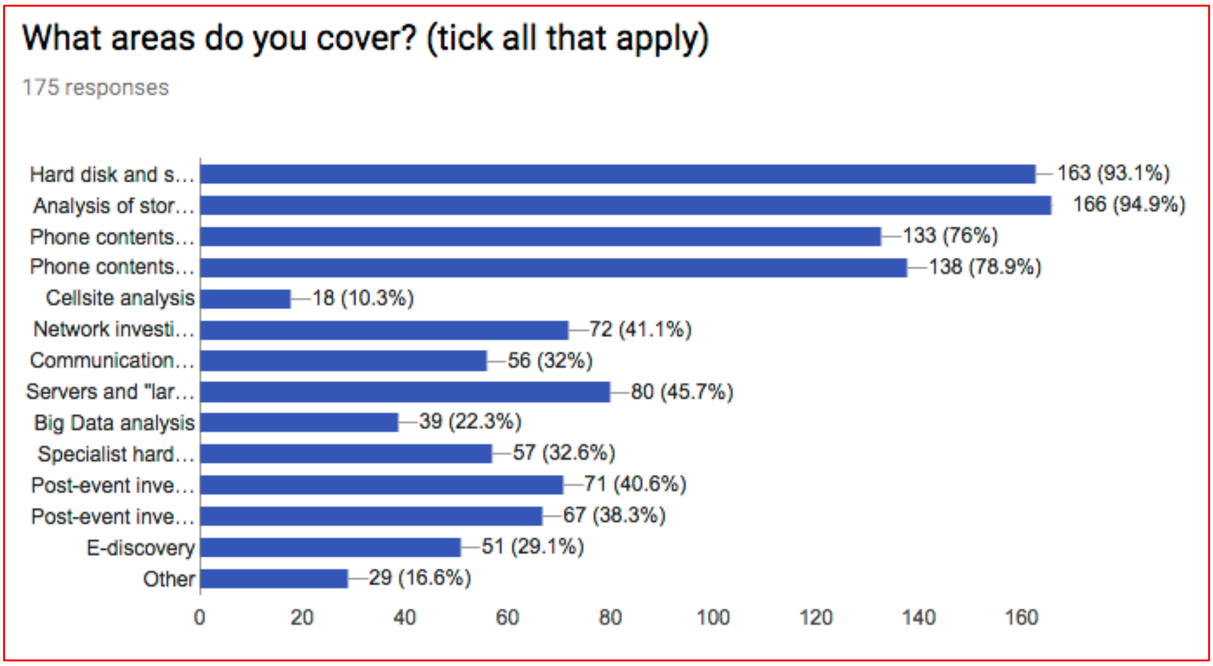
(DF/DE (Digital Forensics/ Digital Evidence) investigator in law-enforcement, DF/DE investigator in private sector with law-enforcement contracts, DF/DE investigator in private sector with no law-enforcement contracts, Litigator who uses DF/DE services, Law enforcement officer/agent who uses DF/DE services, Other user of DF/DE services, Academic with experience of conducting DF/DE investigations, Academic specialising in DF/DE, Other)



Do you (tick all that apply)

174 responses

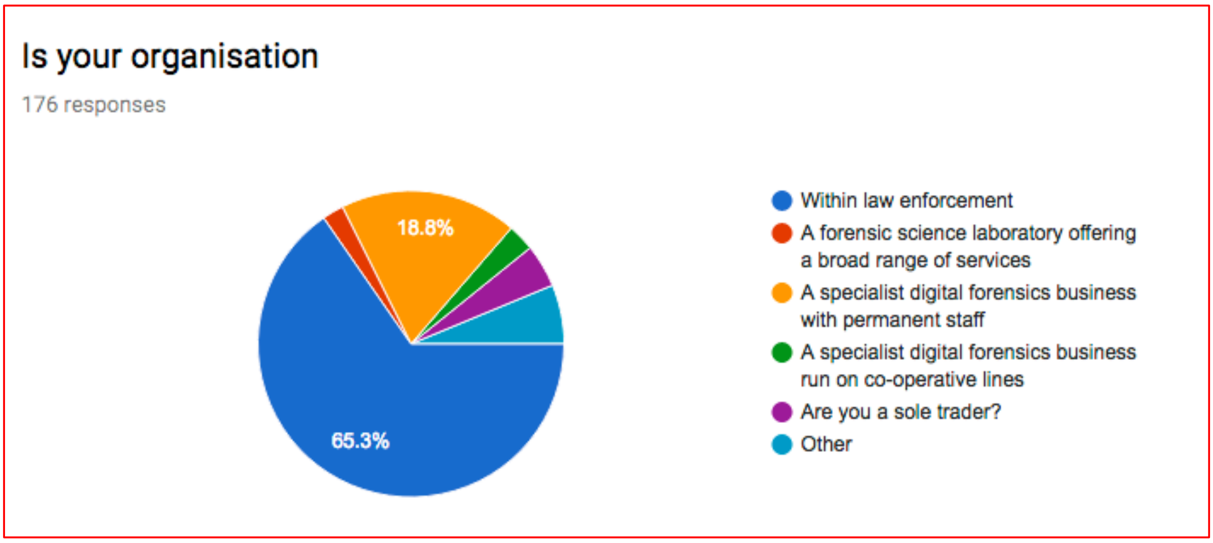
(Work for Prosecution only, Work for Defence only, Carry out civil work, Act as a Single Joint Expert in civil matters, Provide related consultancy work)



What areas do you cover? (tick all that apply)

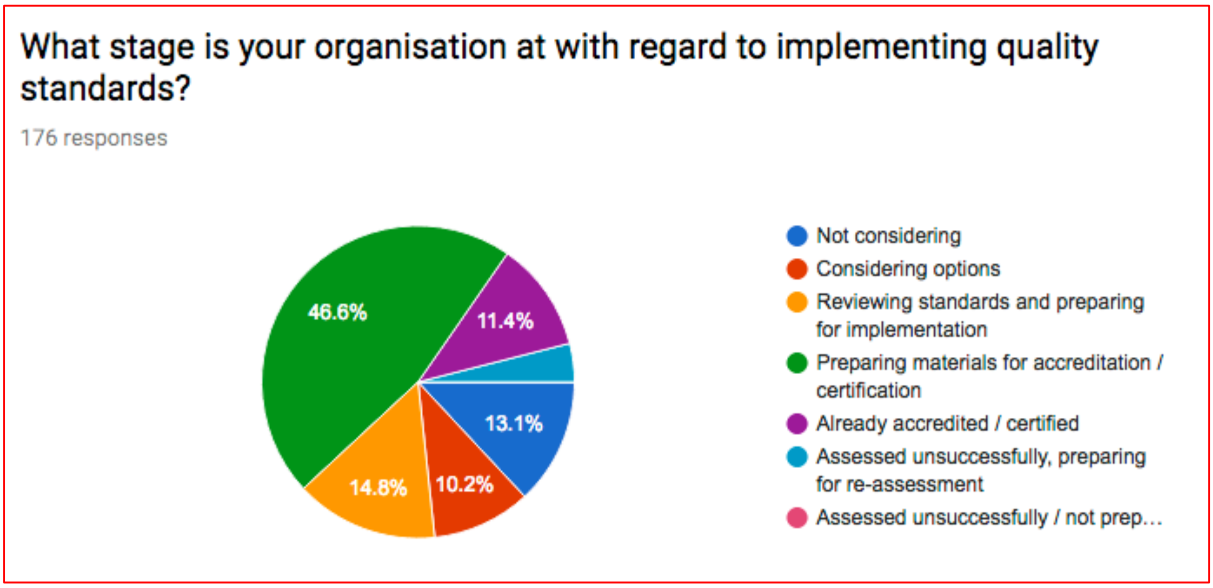
175 responses

(Hard disk and storage media imaging, Analysis of stored data, Phone contents preservation, Phone contents analysis, Cellsite analysis, Network investigations analysis, Communications Data analysis, Servers and "large" systems analysis, Big Data analysis, Specialist hardware analysis (including "chip-off"), Post-event investigations - unauthorised access, Post-event investigations - malware analysis, E-discovery, Other)



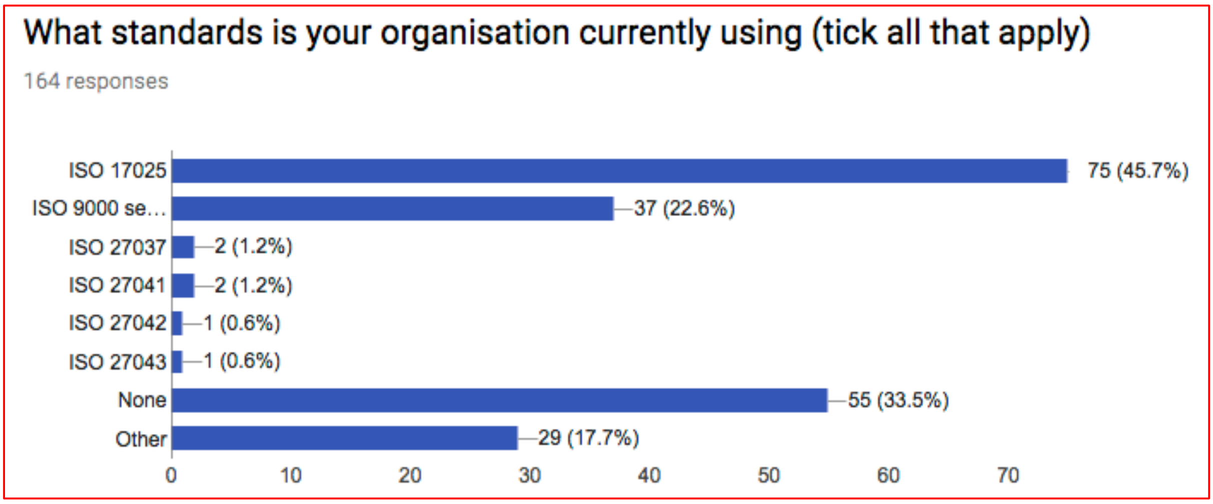
Is your organisation

176 responses

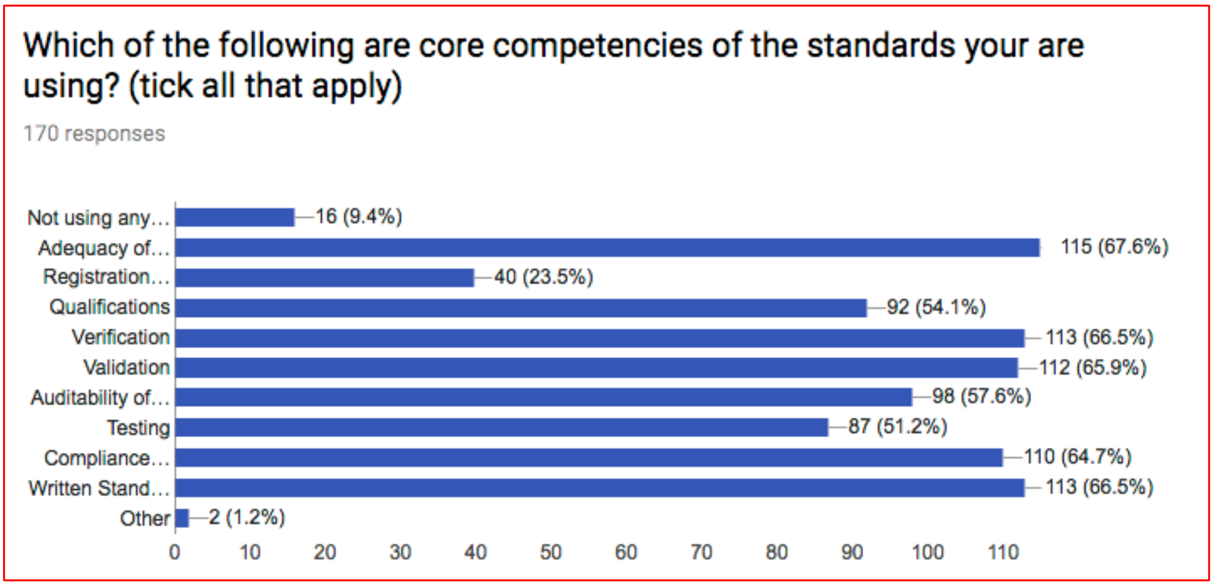


What stage is your organisation at with regard to implementing quality standards?

176 responses

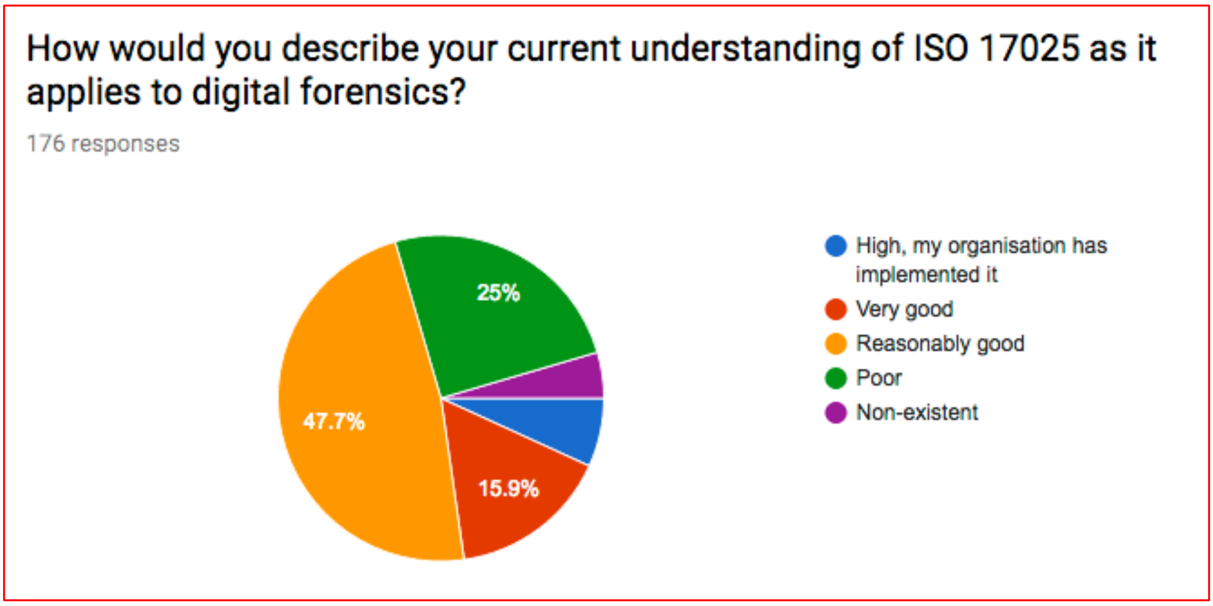

What standards is your organisation currently using (tick all that apply)

164 responses

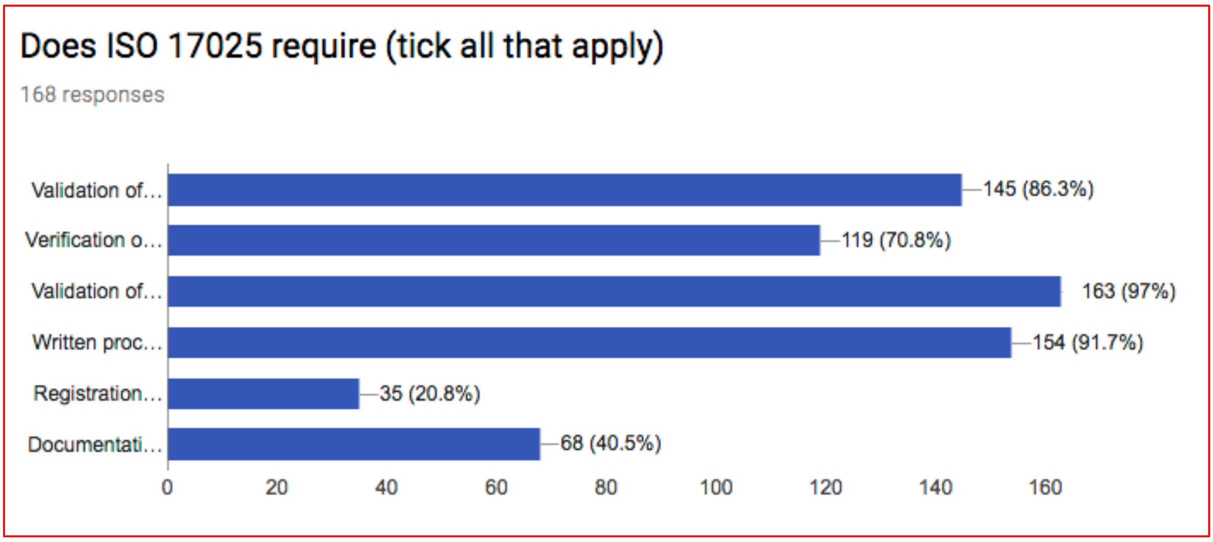

Which of the following are core competencies of the standards your are using? (tick all that apply)

170 responses

(Not using any, Adequacy of Training, Registration with recognized independent body, Qualifications, Verification, Validation, Auditability of Activities, Testing, Compliance with established Good Practice guide, Written Standard Procedures)

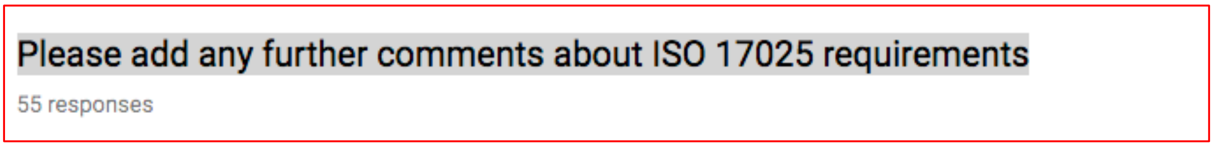

How would you describe your current understanding of ISO 17025 as it applies to digital forensics?

176 responses


Does ISO 17025 require (tick all that apply)

168 responses

(Validation of tools, Verification of tools, Validation of methods / procedures, processes, Written procedures, Registration of individuals as opposed to laboratories, Documentation to demonstrate exclusions from accreditation)



Please add any further comments about ISO 17025 requirements

55 responses

Unsure whether it applies to civil work,

It is too expensive for us to implement and is no guarantee of quality (given recent reports we've received from ISO acredited suppliers).

The mass duplication of effort involved in every digital forensic lab in the country simultaneously and independently preparing for accreditation seems an unconscionable waste of public man-hours at a time of austerity. Why one single UK-wide body couldn't have been given the task of validating forensic tools, which could then be rolled out to all labs, is beyond me.

I've not ticked any of the above boxes because I believe they shouldn't apply. I've worked in a previous high tech unit that was pursuing ISO17025 as a whole, (rather than just imaging) and have considerable experience of it. I strongly believe ISO17025 will offer no guarantees of quality in this field. Whenever evidence is challenged it is never to do with written procedures, methods of acquisition, tools used to examine data and validation of processes, equipment and software. It is always to do with interpretation of that evidence. Just because there is a challenge doesn't mean the interpretation by the prosecution was wrong.

i am at a loss to see why it is actually required. We have well established rules of evidence which when applied correctly maintain a high quality of evidence. ISO appears to be a money spinning scam created by individuals who clearly have now front line experience in Digital Forensics and presenting evidence in Court.

The cost of gaining and implementing the standard will put small businesses (more offices than laboratories) out of business.

not fit for purpose and does not create any benefit over what is already 'good practice'. UKAS have been extremely unhelpful and vague!

You can't apply wet forensic requirements to digital forensics

ISO 17025 is simply not applicable to Digital Forensics.

Should stop at imaging

ISO 17025 is NOT compatible with forensic investigations, It causing more issues than solutions and adding to the backlog which was reducing before ISO 17025 was introduced. I feel 17025 is hindering the forensic process and needs to be reviewed.

It is an unnecessary implementation and will slow down forensic examinations

Resource and time intensive

i feel that the individual should proven to know what they are doing

The "gentleman's agreement" UKAS has with other EU AS means one cannot shop around on price. On the face of it the "gentleman's agreement" is illegal under the Maastrict/Lisbon Treaties.

It has improved the quality of work and improved processes at the two labs where I have gained 17025

Bureaucratic nonsense

Far too onerous, bureaucratic and simplistic

I was originally very sceptical about the value of ISO 17025 but as I have found out more about it and moved towards implementation I have become convinced that it is the only way forwards. The only change the regulator is going to make to the current situation is to make accreditation a statutory requirement - something which will be more likely if people keep moaning.

ISO stifles initiative and innovation.

Validation of procedures would in the course of it validate the tool

Not fit for Digital Forenscis
Not fit for purpose. Not a useful guideline.
Not fit for purpose.
The requirement to adhere to strict ISO 17025 standards in an area of investigation that changes and adapts constantly cannot be covered by a standard depicting 'one known method' of examination. It does not suit either the organisation or the accrediting body.
I do not feel that this adds any value to the results produced by my department. It is just unnecessary red tape with no benefit. Attempts to meet validation criteria have resulted in 2 staff working full time to meet accredition, and only 2 left to do the examinations. Meeting validation requirements appears to involve jumping through hoops with no added value in terms of quality of process. WE are currently only looking at imaging of hard drives. I do not feel that validation of phone examination processes is possible in any meaningful way. There are too many different phones, too many variations in software, and far too many apps -all of which again have different versions. It is only possible to validate this by simplifying the secenario to the point that it becomes completely meaningless - eg validate a phone model that only does calls and SMS, when in reality most people use smart phones with multiple apps.
As with all application of real-world things to a computer environment, there are significant difficulties in translation. Most of the principles of 17025 from wet-laboratories to digital are lost in translation. There is a lack of understanding of the differences between computer science and the real-world science on the part of the FSR. This lack of understanding begins at the use of 17025 as a standard for a digital lab in the first place, and continues through the application of its standards.
Not written with Digital Forensics in mind, or with an understanding of the intricacies/uniqueness of Digital Forensics.
structured and documented processes and methods
FSR were unable to provide direction as to whether 17025 or 17020 were most suitable to our work. We were advised to 'just apply for one of them to show you have quality standards'....
Various implementation requirements appear to have come from traditional forensics and are incompatible with digital. Also, the costs associated with certification are simply impossible for our small lab.
It doesn't fit into digital forensics, it needs its own specialized iso
Over complicated and almost impossible to properly implement
Whilst I agree with standardisation and use of scientific methodology, there appears to be a lack of understanding from the FSR's stance that Digital Forensics is purely Lab based, where a single test can validate a method/process/tool. The attitude that a Digital Lab needs to be more akin to a standard Forensics Lab is flawed. Computers, Networking and IT are a product of an engineering environment, where multiple variables can influence outcomes, in subtle software differences different tools are required for different situations. Relying on a small number of validated tools can be too restrictive, and the regime for constant changing time consuming. With Digital Forensics you are not bring a discrete exhibit into a controlled environment. You are effectively dealing with a dynamic crime scene, and whilst you can control it to some extent, you need to be flexible in your approach and investigation, in this respect ISO 17025 is the wrong standard, whilst still not ideal ISO17020 would be more appropriate. There also needs to be more integration with existing ISO Cyber Security standards concerning Digital Forensics being developed ISO/IEC 27037:2012, which follow industry standards from NIST (who in respect of Digital forensics heavily reference ACPO principles). I would suggest most commercial providers will follow this standard as Cyber Security is commercially more lucrative than Criminal Justice work, and ISO27K will be the standard that potential customers will specify.

I feel the requirement for ISO17025 for Digital Forensics is in the main a standard not directed towards the field of Digital Forensics. The areas covered are included in the main in ISO9001 and ISO27001. An accreditation in ISO27037 would seem more realistic if it was available.

Not necessary - Expensive Beuracracy that proves nothing

ISO 17025 does not provide clear requirements for Validation and Verification (V&V), hence implementing these is problematic. Also, Section 5.4.5.3 of the Standard states that the range and accuracy of values “shall be relevant to the customers' needs”. Hence an element of systematic bias is introduced into the implementation of the Standard.

It requires validation of hardware as well as software. Currently, our write blockers are being checked.

The tools that we use are validated by external companies/bodies such as CAST before it even gets to our lab. Due to this, if there were to be any issues relating to the above highlighted in court, then we would ask the company to account for it on our behalf (that's another reason for doing the training). Therefore 17025 is a pointless exercise form that perspective. 17025 (as far as i'm aware / led to believe) also covers the calibration of the tools we use for 'repeatability', meaning if someone else was to repeat our steps, that they would get the same result, and that the hash value is correct. Due to hard drives failing, the fact that we may have to boot the machine live after acquiring, and that we don't always know the hash of the source before starting the investigation, again its pointless. also if any of the above issues become apparent, we have and always have had the ACPO guidelines to cover this to ensue a fair investigation.

ISO17025 does not fit around a digital forensics laboratory!

No comment

Not sure about registration of individual question - as part of CPR 19 now must be stated that you comply with independent codes of practice which require registration with a professional body.

I have had very little input as to what ISO 17025 actually means in practical terms. From what I can gather by asking around is that it is going to be very costly and is unlikely to yield any better results.

Currently not suitable for mobile phone forensics

I believe this standard is appropriate for Wet Forensics and therefore shouldn't apply to Digital Forensics

Strikes me that the software vendors should be tasked with ensuring their products conform, rather than umpteen labs testing the same piece of software which is prohibitively time-consuming for small companies. Validation through the use of multiple tools and reviewing the data at a lower level should be the goal.

Needs a central government approach to make all companies do the same thing

in a large organisation it is a good route to funding training and equipment at a time when funding is tight

I don't think 17025 seems to fit with CCTV processing. The scope is too vague.

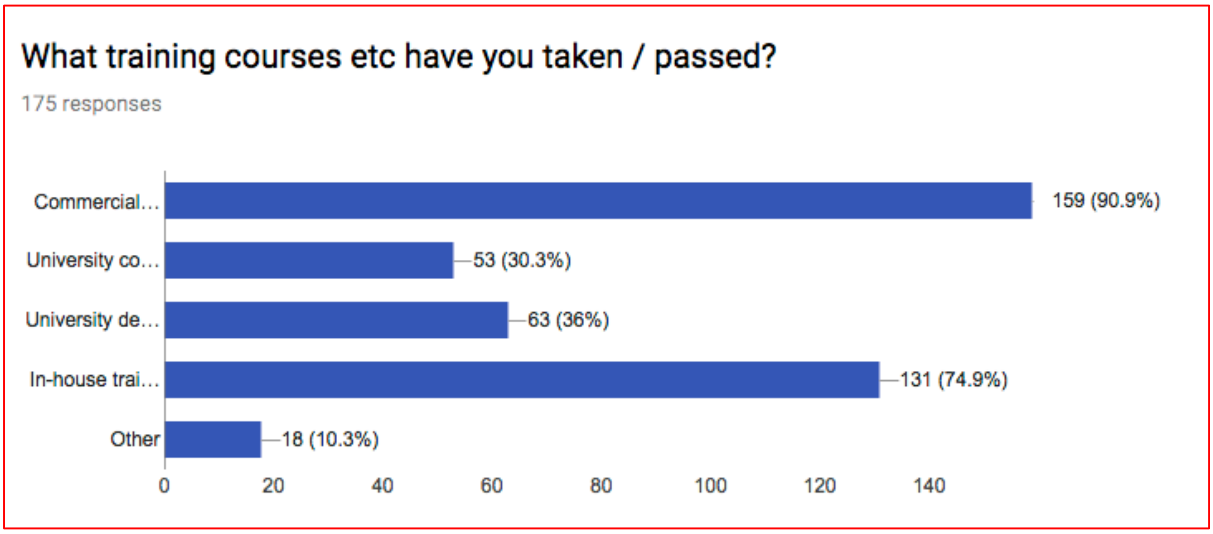
It is the wrong standard for digital forensics

Documentation of staff training, competency testing.

ISO 17025 focuses very much on the idea that a "sample" comes into a laboratory and a "process/method" is applied to it. At the end a report is created. Its a very linear system

I find it an infuriatingly inadequate fit to Digital Forensics. It is stifling the field without providing any actual guarantees of improvements. It is a drain on resources of already over-worked Police HTCUs. It is a barrier of entry to any private contractor wishing to provide DF to law enforcement, meaning only the very big companies can compete.

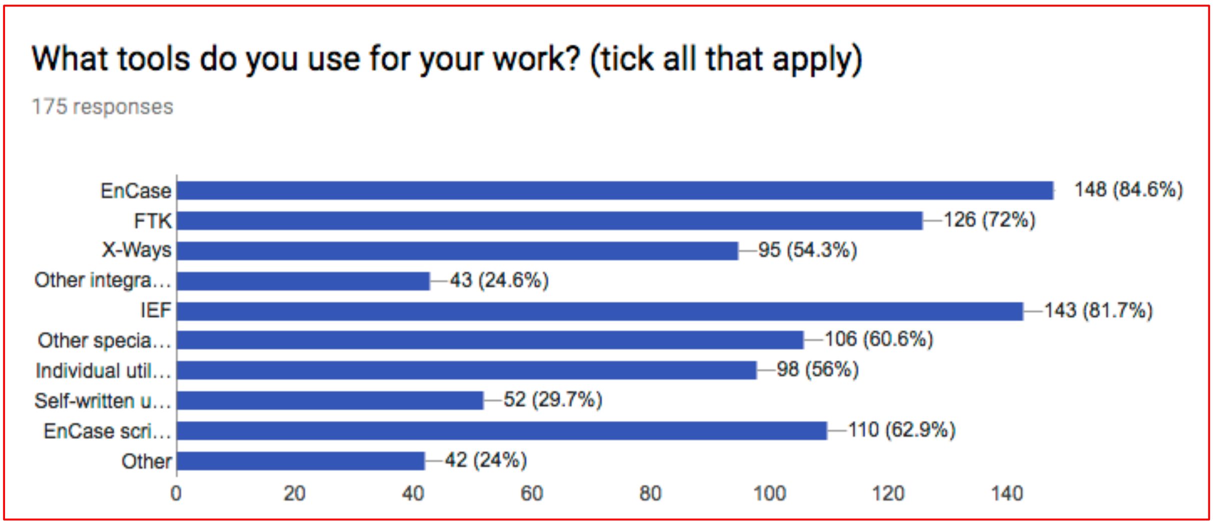
Some requirements seem needless. The need to hash pictures taken during examination of a physical exhibit. I have never heard it suggested that the pictures were not the originals or that they had been edited.



What training courses etc have you taken / passed?

175 responses

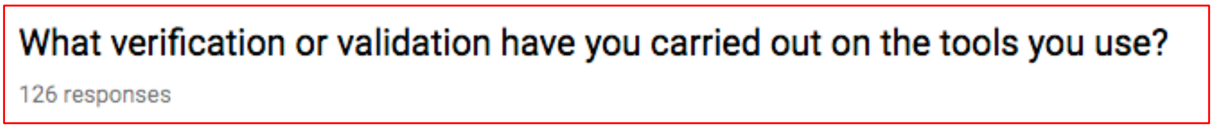
(Commercial courses successfully completed, University course but not resulting in a degree, University course in forensics, in-house training, Other. The survey also collected details of the courses and the associated dates – there were 101 detailed responses)



What tools do you use for your work? (tick all that apply)

175 responses

(EnCase, FTK, X-ways, Other integrated suite, IEF, Other specialised commercial tool, Individual utilities written by 3rd parties, Self-written utility, EnCase scripts and similar)



What verification or validation have you carried out on the tools you use?

126 responses

None
None
none
none
none
No comment
No comment
All thoroughly tested
Dual-tool verification
Numerous
Test against other similar products and against manual extraction/analysis.
tests and verification
Where I have used third-party tools I have in some cases uses the tools to present and refine evidence, but i have also applied either a "dual-tool" approach to the data, or alternatively (and more often) performed an analysis of the raw data itself to ensure that the tool is correctly interpreting the underlying data structures. .
Dual tool verification and other ad hoc testing
I've carried out validation of write blockers, dedicated imaging computers and imaging tools.
I've been involved in creating test sets of data for analysis tool validation. A very arbitrary data set provides no guarantees of suitability of the tool for even newer versions of the same software in that dataset, (and possibly even that version of software if you consider third party programs like anti-virus tools).
Verify using second forensic suite
Write blockers checked before each use.
Validated SOPS and Guidance Notes. These processes needed validating with certain tools by way of verifying that the known data sets were extracted (where declared as supported) thereby also validating the forebsic software/hardware
I validate the results that I produce, not the entire tools as this is simply not practicable.
Use of the TVP image files
All the tools we use for in scope work have been validated to ISO17025
Using a drive with known files
as per iso requirements
Tested Acquisition and Proficiency Tests re FTK, Encase, Tableau, Caine
None yet
n
ISO team have created test data and verified results
Original Manufacturers Licenses. All processes are verified, usually with secondary tools.
Validation and commissioning of write blockers, Encase, Nevis, Griffeye and FTK.
At this point verifying the extraction of specific artifacts such as Windows Registry, Internet Artifacts, Pictures, Movies etc. each in its own validation plan from start of process to finishing (including within a report)
Full validation and verification to ISO 17025 standards
Hardware and software validation.
Currently completing
none yet, only on FTK imager
Usual method, control sample input, check output is correct.

All tools are validated in accordance with FSR & 17025 requirements

verification against a prepared image file with known contents

Very little. Mostly the tools are industry standard and it should not be for practitioners to undertake this work

Verified functionality of tools against known data sources to confirm accurate and repeatable functionality. Validated methods to ensure processes can be applied consistently and accurately.

Imaging I test write blocking after updates. Evidence is dual tooled. Never rely on automated results.

Comparison with other tools and manually checking.

Validation

Dual tool verification primarily where possible/practical.

validated tableaus and FTK imager against Lab prepared test media and attempted to validate EnCase against Lab prepared media

Range of storage devices and elements of analysis - this is ongoing and we are yet to do phones (but have a plan)

Single member of staff conducts all verification and validation

To date - Mobile Phone tools only - Extending scope to PC

retesting at regular intervals against known devices and cross-compare

It has been carried out regionally for ISO 17025. I have done my own testing and validation in the past.

Very little presently

Extensive.

None. To be completed.

FTK Imager Only and CAST Validation on workstations

EnCase images -v- FTK images

Partial manual verification and validation is ongoing. No technique fully formed at this time.

Sourced test data/results from tool manufacturer/developer. Devised method validations for the procedures that utilise a 'tool'.

imaging validation - conventional hard drives

In house testing, which has found the tools wanting, especially Encase.

none personally

Verification of extracted data compared to live data on the device is also completed which would enable other tools to be used to capture a complete data set if required.

None - because I verify my results - not my tools

Core tools are validated based on predicted (or expected) output within specific use cases. Due to the proprietary nature of commercial tools, we have no access to source code and any testing is therefore black box. Due to the complexity of these tools and the unpredictable nature/infinite variations of digital source data, it is impossible to test every possible program path by black box testing. Whilst such lab tests may validate one aspect of the tool when using a specific test disk, a real world exhibit may contain a completely different configuration (e.g. operating system, hardware, installed applications, hardware/software corruption) which will could result in incorrect output. In my opinion, caution should be applied to such tests as validation in the lab does not necessarily prove the tool will work correctly in all future use cases.

Controlled Tests

None to date

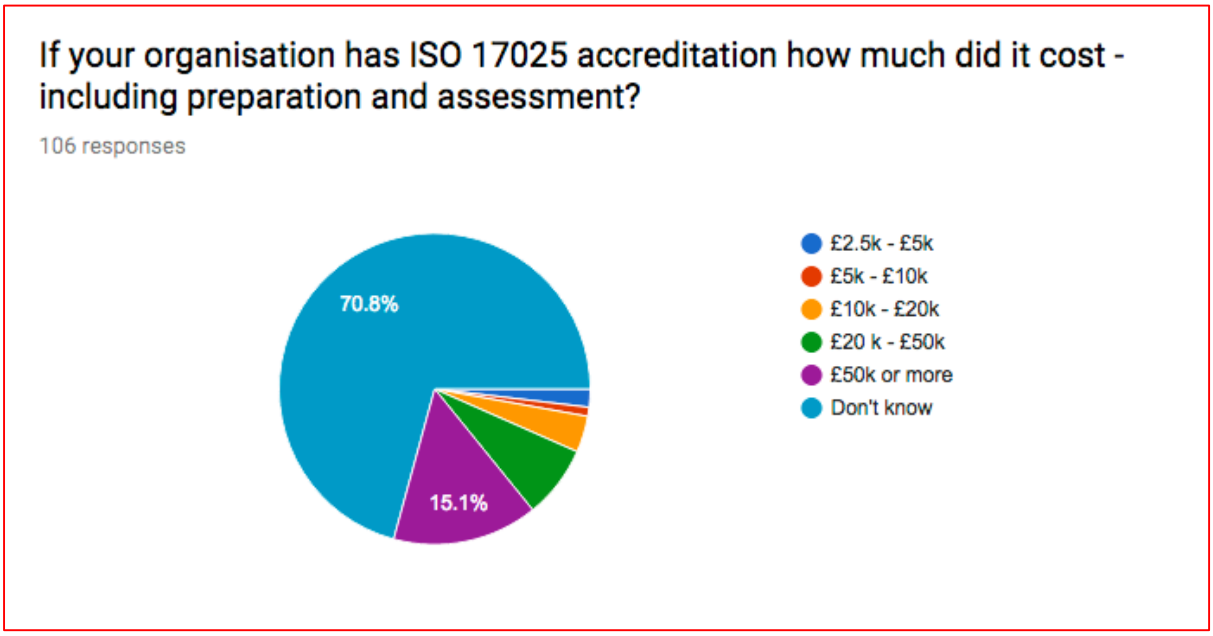
None by ourselves only what the vendor has reported.

no comment

Validated write blockers

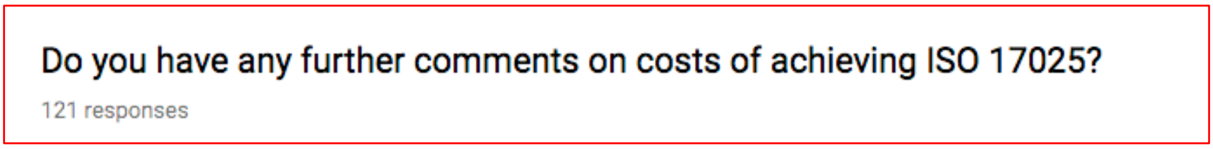
Standardised image with certain artefacts to find.
This question demonstrates a lack of understanding of accreditation and the requirements of the ISO IEC 17025 Standard. The "Tools" are not validated; whereas the "Method" is.....
Continual verification of software by cross examining with second set of tools
Frequent dual tool verification of findings
'Day-to-day' replication verification of tool's abilities and limitations. Validation of methodologies utilising said tools
Test new versions against known data sets from NIST
None. I only use standard tools and do not rely on them to do my thinking for me.
Hash checking
CAST HDD comparison of Hash value for HDD & SSD
Full method validation for acquisition element only
Yes
Dual tool verification
In the process of being conducted
just completed PhD in this area related to use in malware forensics
tool testing of effective parsing of data and interpretation via known data and results
Testing of our write blockers and showing the hashes are not changing. Testing EnCase (keyword searches, recovered folders, encryption to name) by verifying the test data is the same as the original data. C4All scripts with Griffeye. Making sure our reports are working.
as a report writer I have to validate what the tool is telling me at every stage. However we have a dedicated practitioner who's job it is to ensure that all tools (hardware and software) have had a validated test before they are used in the lab.
Periodic validation of findings from one forensic tool with another product.
We have carried out verification/validation of physical hardware (write blockers / imaging devices) and imaging software. We have prepared procedures for testing our main tools such as FTK and EnCase
For accreditation only
Validate results using hex editor software/other tools against a known image created by ourselves.
Full method validation on all tools within scope
None so far
In the process of validating our methods. This will include some verification that the tools do what they are purchased to do. The tool will be commissioned upon purchase and will have a data set with known data used against it.
I always use multiple tools. If I am in doubt or using something I have not used before I will write my own scripts to validate my work.
Standard write blocker verification only.
Validation of imaging tools
In house, populated all devices with data and imaged, extracted, analysed etc.
Only for imaging tools using test disks with known hash values
Compare previous recovered data against new release
none, they are validated by the company's that write them!
In-house verification of generated hashes of captured data.
already validated before we use them
test images for FTK and Xways. Mobile Phone library to test Cellebrite and XRY
Using two tools for each piece of data / artefact and common sense approach to reviewing the underlying data.
lots against known standard data sets
validation on imaging and pre-processing

Comparison with other tools
ACPO best practice guide is followed.
imaging validation of conventional hard disc drives, solid state drives and peripheries
Imaging of HDD, SSD, other storage devices. Decoding for some mobile tools.
Brief testing with sample images. No framework or suitable images can be easily found. ISO is causing confusion on the scope and how to test a suite of large tools such as Nuix.
In house validation. Results often manually verified where possible
currently running tests of methods that use these tools
In-built verification. Dual tool verification of evidence for each case.
Write-blockers are verified bi-annually
this work is carried out by our technical manager
In house testing for imaging tools; in general 'key' findings verified with more than one tool per case.
NIL
Specifically against individual tools - none
Unknown
Validation between the tool sets
Verified successful write blocking and imaging with the TD imagers. Working on doing the same for other imaging tools.



If your organisation has ISO 17025 accreditation how much did it cost - including preparation and assessment?

106 responses



Do you have any further comments on costs of achieving ISO 17025?

121 responses

No
No
No
No
No comment
No comment
If it is any of the figures above, it would cause financial strain.
Too expensive- and not relevant
It is so expensive to achieve, and such a poor indicator of performance and expertise, we will NOT be implementing it and will therefore no longer work on behalf of the Prosecution in DF cases. We already attract vastly higher fees for similar work in civil and privately-funded work that there is absolutely no financial benefit in us implementing this.
This ISO is financially unviable for a small company
Far too expensive for me. I am essentially a small business - a "one-man-band" - and the cost of accreditation is way beyond what I can afford either financially or in terms of the time which I would have to expend.
See above comments regarding duplication of effort.
My previous department unsuccessfully applied for accreditation. When considering the costs of salaries of dedicated quality managers, (which we didn't used to have), the loss of time for each analyst in conducting validation and completing extra forms, I would say the process cost well in excess of £200,000. We did in fact cut two analyst positions to fund two quality managers. I am particularly concerned about cost. In that department almost the entire training budget was swallowed up by costs of accreditation and we also had to cut back on the number of licences we had for some tools where we really need to have one licence per examiner. As

analysts we found our productivity dropped with most analysts doing about 70% of the number of cases per year that we used to complete. The only way to get that number of cases back up was to do a less thorough investigation than we used to do. I don't believe small companies and 'one man bands' will be able to afford ISO17025 and this describes the majority of defence experts. What happens when a defendant can't find an expert?. Considering staged reporting means evidence may not have been validated by an analyst, I think there is a greater need than ever for good defence experts. I believe we will start to see miscarriages of justice.

Punitive.

far far too high!

we have 16 sites with Labs so is massively expensive.

It impossible in the timescale and a major distraction to actually trying to catch criminals

ISO 17025 is simply not applicable to Digital Forensics.

Its is achievable but not easy or simple and needs the right approach by the team undertaking it

Waste of money and time

Non profit organisation UKAS extortionate expense

Proficiency Testing is very expensive for what it is (used ISFCE). Whole thing seams like a cash cow for UKAS etc.

Very high including on costs

money could be better spent. waste of money and time

all satellite labs required environmental changes and staff abstracts take the cost into the 100's of thousands.

The cost will make it prohibitive for me as a small private business. This is very frustrating as I provide a service that produces evidence that has been acquired within accepted practices and is admissible as evidence in the UK judicial system

No comment - I am unsure how spending is managed

They appear to be very high, requiring standardizing of a lot of hardware and software as to make sure validation and verification can be replicated on all hardware with the same software on each machine.

Very Expensive to implement and unnecessary, we document what we do so others can verify this if required and always have done, so I don't see the point of ISO 17025.

Exorbitant

It cannot cover all fields of expertise before the Court. The proper test is independent peer review of all expert evidence to be presented to the Court long before the trial date. "Independent peer review" is not another member of the same firm simply ticking off a report but the "other side" reviewing it, prosecution expert reviewing defence reports and vice versa. ISO17025 cannot achieve that.

Expensive but worthwhile for ensuring quality work

waste of resources

For some forces/bodies the cost will be vastly inflated by the need to outsource in order to free up internal staff to undertake ISO work. The cost of this over the entire country may well run into millions.

It is an incredibly expensive standard in terms of the costs associated with assessment and the abstraction of man hours.

I feel that with the work hour required to achieve this accreditation, it will not be achievable for all and will not be sustainable for most.

The cost of achieving and maintaining it looks over the top for small forensics departments

it's rediculous

It is potentially going to cost (including developing the system) somewhere around 30K, probably more. As a result of the expected impact I have merged with a larger Cyber Security business who are investing. I think the days of the small one or two person business are over.
The figure above says everything!
The costs are prohibitive for most non-government/law enforcement bodies.
I have been doing computer forensics for 17 years and have MSC. most of the ISO17025 is a waste of time when resources and funding is stretched so much. There are some aspects of our work (archiving, CPD, policy documents) which have slipped over the years due to work loads which are now having to be revisted.
Reduced productivity
no not involved.
The time cost, the lack of clear guidelines and its unsuitability for the field do not make it worthwhile to implement.
After cost saving measures have been implemented, ISO17025 seems to be bringing in more and more therefore costing more money.
I cannot for the sake of me understand the need for this standard for Digital analysis. The term Forensics should be dropped and therefore come out what is required for labs. This area is completely different to science labs, DNA and fingerprints. This is costing a huge amount of money and time across all 43 police forces. The forces are completing their own pieces of work on the accreditation and all are different in their ways. We should be able to get uniformity across law enforcement as we did with ACPO Principles so that nationally we could all work to best practices. People are making loads of money from this adventure and not focussing on bringing Offenders to justice and safeguarding the communities we live in.
Time impact will be huge and the quality of the 'product' is a visage. ISO standards does not improve the quality of the analysis as It's less likely that an examiner would take an R&D approach to extract and analyse the data on mobile devices. You are more likely to create a 'factory - of - people' that mind numbingly follow the ISO processes without cause and consideration for what they are accomplishing.
It is a constrictive cost to a commercial FSP and one that can easily be underestimated. Grants and/or tax relief should be made available.
not sure how much the total cost will be.
Lots of the costs are hidden.
None
Would be far betting spent on preventing and detecting crime
Time prohibitive per device, length of time needed to produce data and complete validation of tools.
Cost is difficult to measure as it has been a part time requirement of all staff. The more significant cost is in the investigations that have not progressed because of the pressures of ISO.
Not affordable and effectively puts me out of business. Most LE agencies I come into contact with have two or more people working on ISO17025 compliance full time. How does a sole practitioner achieve this?
High cost for a small unit with limited budget and will effect funds available for department including forensic training.
We believe it to be cost prohibitive
Not specifically involved in the costs, however from what I've been told it seems like a costly process, especially for government departments where budgets are continuing to be cut.
It seems senseless that that 43 or so Police organisations are individually trying to write process and procedures to satisfy a adjudicator who appears less qualified than the practitioners that are practising within the field. Many thousands of pounds of public money

appears to being spent. I would suggest a Freedom of Information request and a scrutiny by the Public Accounts Committee may well reveal what the cost is to the public purse.

very high as far as I understand, impacting many small businesses.

Way too much for small units like us

The current figure for the Acquiring and Exhibit handling will be approximately £200k+ be the time the building, equipment, abstraction from duties, meetings, cost of accreditation are taken into account.

It is worth the effort and cost as standards in forensics is essential.

prohibitive on a small company

Stupidly high

Waaay too expensive!

I have estimated that it will cost me in excess of £70,000 to implement and approximately £40,000 per year to maintain

Significant costs in personnel time from both a managerial and practitioner perspective. Whilst some of this is a "one off" set-up cost there is an ongoing obligation which add significant overhead to each case. Considerable outlay in purchasing additional equipment; e.g. test handsets to validate data against.

ISO 17025 would cost more than my turnover and would be entirely irrelevant to my work. I would expect that it would give similar difficulties to other sole practitioners and those who specialise in working for the Defence. Not all work is laboratory work.

Extra staffing costs over 60k per year, training costs £360k, new equipment 100k

Its a high learning curve

If I was a cynic this is a deliberate attempt to squeeze the provision of Digital Forensics out of the Law Enforcement onto a purely commercial basis, into large companies. This will mean only large companies would be able to provide Digital Forensic services, at a time where Computer based evidence and criminality is becoming the new volume crime, touching most crimes occurring today, therefore access to such services need to become more common place, easier to access and cheaper - this is having the opposite effect making it more expensive, used for only high level serious offences.

Unrealistic for small enterprises with return of costs not being covered in the same work being completed.

the current cost is not financial but in time lost and nonsensical directives overriding common sense

Wasting a lot of Analyst's time writing, checking, validating, and verifying written procedures. Adding extra workload to an investigation, and slowing down case processing times.

Have no intention of implementing it

The costs are being taken out by us not just buying new equipment but staff time as well. Staff time = less time on cases (Could be an impact on Law Enforcement)

I have not been given even a rough figure of how much it has/will cost as its not for me to know.

I believe the costs are totally disproportionate to the benifits that ISO accreditation will provide. We have already written off one full time investigator and two support staff in its preperation for up to 18 months. Much of it is to accredit processes such as forensic imaging tools, and yet, when have we ever been challenged in Court? It is either a verified forensic image (hash value) or it isn't.

We are currently in the process of gaining our 17025 accreditation. The costs involved are high and in my opinion unnecessary. Any forensic examiner should be checking their work at fundamental levels rather than placing reliance on tools.

No Comment

I have done some research into the costs of achieving ISO 17025 and we as a company are weighing up the costs/RoI.

The only additional costs are the assessment fees, everything else would be part of running a proficient DF lab with/without 17025

Forever growing

With recent legal aid cuts and hours granted by LAA being strained, it is not in my view achievable for single practitioners who still have a passion to work within the criminal sector and work in multiple disciplines. We are already struggling to make a living out of it and if we don't work on cases we don't earn anything. Hence, it isn't just the actual costs but also the large loss of income and research time. I work in the evaluation of phone content evidence, connection record analysis, cell site analysis, attribution evidence with respect to phones and then full computer forensics from a USB up to servers. I'd be constantly working on getting accredited in each of the areas and not actually working on cases. I also work in specialist cases at times testing software/systems/procedures to determine their functionality and/or interpret data. I doubt the LAA would grant me funds to write bespoke procedures for these cases - it would likely cost more than my actual work. I also sometimes turn up on a site without any prior knowledge of the system I will be testing.

Believe the costs could be spent elsewhere, especially in cash-strapped Police Forces

£10, 450 so far.

Too much

Excessive and the organisation having to pay s verbal times for different disciplines

It is a considerable amount and increasing.

It is a ridiculous expense for a process that should be centrally rolled out and funded. Why should police pay to be a prosecution agency, and 100s of thousands of pounds to get a badge is a nonsense

There have been no indications from the regulator how much ISO 17025 would cost to implement. This has made it difficult to raise business cases for extra resources, so implementation is being done on little to no budget.

Cost is prohibitive to Small Private firms,

We previously held ISO 17025 and the costs were expensive

It's costing way more than it should given the amount of examination hours lost from preparing for ISO and reading documents, signing a document to say we have read a document, then that document changes so we need to re-read the changes to the first document and sign another document to say we have read the changes....

na

Estimated cost for business, decided it could not be justified without guarantee of additional work to cover costs. Moving away from law enforcement work as a result. A real shame.

I assume the costs are astronomical in departments / forces attempting to acquire accreditation and then once acquired to maintain it.

Wasted money in my opinion.

It is far too much work and far too expensive. It will lead to the demise of small organisations for no obvious benefit.

Yes unsure.

It is expensive and has ongoing costs

very expensive

Considering the budget cuts and pay freezes on front line functions, it's hard to accept this is the best use of money.

Too expensive, monopoly held by UKAS, massive cost hit to efficiency due to overheads

I'd much rather use it for additional staff training, equipment etc.

no comment

Prohibitive and unrealistic. There needs to be more done with industry to make this more viable.

Very high for what it is, requires additional staff to what we currently have

Organisation has underestimated the resources required to achieve accreditation

Our initial assessment by UKAS has been quoted as costing £21000. This is on top of all the man-hours we have wasted with SOPs and documentation.

Being a team of only 3.8 FTEs, the cost is likely to be too expensive for this department to bear.

n/a

Would only consider it viable if paid for by the employer. Seems very difficult to achieve as a sole trader, should I find myself in that position.

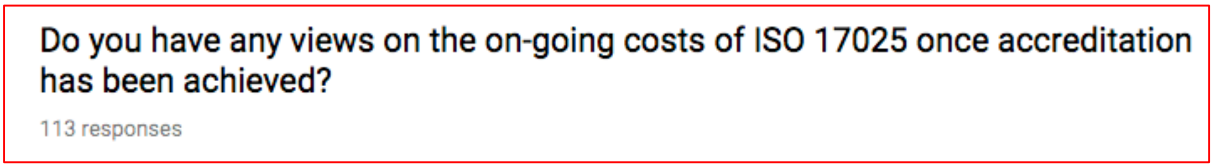
It is an expense that nobody needs at the moment and will prevent sole traders or small businesses from being able to work with LE

Very expensive!

Resource intensive

N/A

Costs seem excessive and likely prevent smaller organisations or individuals from obtaining the standard.



Do you have any views on the on-going costs of ISO 17025 once accreditation has been achieved?

113 responses

no
no
no
no
no
no
no
No
No
No
As above
As above
None
None
See above
See above
No comment
No comment
Nome
Too expensive- and not relevant
This ISO is financially unviable for a small company as a annual cost
Again, far too high.
I think the cost of maintaining ISO17025 accreditation will mean reductions in budgets for software, equipment, training and staff numbers. Staff will spend less time on each case because there will be fewer staff and they will have more 'admin' to fit into their working day. As I say earlier I don't believe 17025 offers any guarantees of quality but it will mean less money for things that do improve quality.
Shockingly expensive
Far to expensive.. in a time when police budgets are shrinking we are spending £100,000's on accreditation. This could pay for police on the streets!
The cost of ISO 17025 is simply ridiculous and if the public became aware of the cost when compared to the results they would be outraged. The standards in my organization are extremely high with full verification of our results. The ISO standard has simply complicated the already difficult process, causing significant delays and taking large quantities of public money.
Force has no budget for 17025
The whole thing is too costly
It's not an area I get involved with
If its acheived
Prohibitive for all organisations
Too expensive and too much work involved to keep it maintained.
The on costs are a ridiculous waste of public money
the cost to the public purse and affect on service delivery over the last few years is concerning
Unnecessary bureaucracy
No comment - I am unsure how spending is managed

The upgrading of hardware to meet the best practices could be expensive, and with buying one forensic machine costing so much, buying 14 (in our case) every 3-4 years can prove very expensive. It also creates a waste of computers that are well within lifespan still.

It will be an ongoing process which will cost a large amount to maintain.

higher than is necessary, with every software release, further validation will be required and we use easily 10 tools that will need validating, someone could easily be employed full time just to do that

Acquiring 17025 is not easy however maintaining it is very time consuming and therefore expensive, its a full time job.

as above

Monetary costs at times of severe financial constraints should be avoided if possible. On-going costs will eat into budgets that would be better spent on efficiency/staff etc.

I believe it will remain expensive to continue accreditation, again due to the ongoing staff costs associated with performing the required audits, competency tests etc...

yes

see answer above

For the first few years they will be considerable because we will be doing scope extensions every time, then it will settle down a bit.

Someone is making a lot of money out of ISO, so I can't imagine the costs reducing...

Again, very prohibitive.

Money way better spent on modernising equipment and training.

Lack of future innovation and slow take up of new tools.

no not involved.

As above, not worth it.

Again the cost to maintain the accreditation and for people to be taking away from what they should be doing is vast. This matter should of be dealt with at a national level sooner. This 17025 is too stringent and not necessary. I have to my knowledge been aware of any miscarriages of justice in our force. With defence teams checking evidential work they have right to challenge at court.

Yes - it's immoral.

For our company, it will be a significant yearly figure requiring several full and part time administrative positions. The increased staffing costs and extended operation time will have to be factored into the service costs to the customer, which are expected to increase between 10 - 25%. Consequently, it is imperative that the FSR enforces the ISO standard requirement.

It will be expensive.

Way to expensive - just in terms of man hours the cost will be enormous

Maintaining the validation and verification of updates for software and hardware tests.

Maintenance appears to be such a burden that there will be a continued cost to investigations

Not affordable as a sole practitioner carrying out mainly LSC funded cases

Will effect funds available for department including forensic training.

It is going to be a increasing cost to the organisation and tax payer.

costs required for reassessment when required

unknown

They are unreasonable

Surely a more nationalised approach would have been useful? Whilst I agree, standardisation is useful, as a member of public the extended time taken to examine and the potential additional staff we could have had would have been more useful

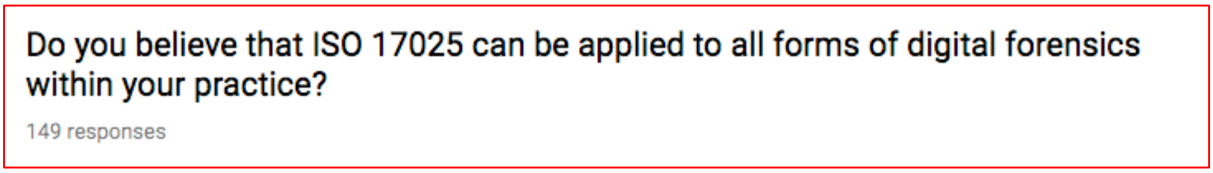
prohibitive

Stupidly high

My business will probably close

On going costs will be significant as the overhead it introduces will slow the workload that a practitioner can achieve.
It's not value for money.....our evidence still needs to be validated and tested by the court system. UKAS are no replacement to the CJS.
Unsustainable
didn't know there were on-going costs
Adding extra workload to an investigation, and slowing down case processing times.
No see above
would like to hear
The ongoing costs will be higher than what it was before without the standards. It will secure more training which is great.
No for same reason as above. However I would envisage that the costs could be forever increasing as the 'needed' quality standards increase that we have no control over.
Here again in the climate of reduced funding certainly in the public sector this can only take funding away from actual safeguarding casework and examinations.
For a not-for-profit organisation UKAS is very expensive in my opinion.
No comment.
The main cost is the assessment fees. Our initial assessment cost £22K for 3.5 days of assessment. This is very impactive as an assessment is required every year
Keeping up the standard is going to be difficult and extremely time consuming.
See above - it is not in my view achievable for single practitioners especially those working in multiple areas.
Again, money that in my view could be spend elsewhere
I'm not sure that the vast amount of money and effort is going to achieve better results.
Too much for the result
Will be factored into yearly budget
Yes, it is not acceptable for UKAS or the forensic regulator to have no concern or consideration as to how much public money is being spent on this.
Should be centrally funded at least for those who achieve the grade
there is a business concern regarding the costs and whether or not we will continues if 17025 becomes compulsory
Too Expensive
Too expensive -
na
I know CCL have personnel dedicated to maintaining the accreditation. The costs must be very high
See above.
Absolutely too expensive
difficult to budget for
It seems to still remain costly to maintain.
too expensive, too many overheads
Too expensive, tick box exercise.
no comment
Again, prohibitive - businesses cannot sustain this accreditation at the rate the industry is going. A race to the bottom for law enforcement and legal aid, no funding from government, and the increase in expert salaries and costs means that the ISO standard cannot be sustainable
Going to grow exponentially if all processes have to come under ISO
Organisation does not understand the on-going impact keeping accreditation will have.
Absurdly high.

Full on-going accreditation would most probably lead to the closure of the team.
n/a
no views
Very expensive!
Only resource to provide upkeep of records etc
We need to recruit a Quality Manager and a technician due to ISO 17025
N/A



Do you believe that ISO 17025 can be applied to all forms of digital forensics within your practice?

149 responses

No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
no
no
no
no
no
no
no
no
no
no
no
no
Yes

Yes
Yes
Yes
Yes
Yes
No.
No.
No.
No.
No.
No.
yes
yes
yes
yes
yes
Yes.
Yes.
Not sure
Not sure
No - we are not a "standard" company delivering "standard" solutions
No, and it would be a waste of our time to try.
It is a total waste of time
No - In fact i don't think it can comfortably be applied to any of the forms of digital forensics within my practice.
Absolutely not. We deal regularly with volatile data on unpredictable systems, where our actions have to be chosen by risk assessment rather than by rote procedure.
No. I don't see it as beneficial in any area of digital forensics. I think other standards are more suitable or 17025 could be used as a new set of good practice guidelines. Although I haven't been involved in chip off/chip on work, I do see that as a potential area for 17025.
Digital - computer forensics is a challenge but possible. Digital video is proving to be very difficult
I do not think the standard applies to all parts of digital forensics. Take the examination of mobile devices for example, they move at such a pace that trying to verify a complete tool to examine all types of phones is simply impossible. However, ISO is causing us to use a standard for the sake of it even though it has no hope of achieving what it is designed to.
Yes, at a cost and a lot of time
It could but why should it
To a certain extent but there is so much which can go wrong with a computer process and a lot of testing and trying different things to get it to work. ISO doesn't lend itself very well to this without creating a none compliance.
Not a chance
Leave it at imaging
Not in its current incarnation. Digital Forensics have been shoehorned in to traditional forensics because UKAS/regulator doesn't understand.
I hope not!
Not at all. Data Forensics is an ever changing world with no two computers the same. ISO is designed for a standard process. There is not flexibility and creates more work than needed.
Not all, simply because of the fluidity of digital evidence and how more artifacts can be discovered but have to be performed under ISO guidelines, under my understanding means we

almost have to ignore the evidence until we have a proper procedure to show what we have is accurate.

Yes, but not necessary, and very time consuming, we have 4 people working just on ISO 17025 and it's draining our team massively.

not suitable where tools and processes change very often

Yes, seven years ago I would of said no but having lived with for so long and worked with it it does fit Digital Forensics.

No the standard does not fit with DF and was badly chosen

I think losing several staff to accreditation activity vast swathes of time does not represent good value in the public sector.

Absolutely not.

It was difficult to apply to a predominantly e-discovery focussed lab that mainly works in the civil arena. The UKAS assessors often struggled to understand the requirements of our organisation, which required considerable effort to repeatedly explain our operations and the legislation we work to.

No - 27037 is the better standard for Digital Forensics. 17025 shouldn't be shoehorned to fit when there is already the exact standard existing.

I believe that it can, but it may change the methods undertaken and can hamper potential future improvements.

Not easily in a realistic cost effective manner

it will have to be.

Part of the process is developing a means of performing non-standard process and some activities will probably remain outside the scope of the accreditation however the overal process will include these, with appropriate caveats and statements of uncertainty.

No. We encounter new technologies every week that we are expected to analyse for evidence - drones, car telematics, smart watches etc. ISO is not fit for purpose to all forms of digital forensics.

No....

I dont beleive that 17025 is a good fit for ANY digital forensic practises.

No. I can see how it works for DNA / Fingerprint labs, but definitely not computer forensics. Nothing ever stays the same in the computer and mobile phone world. Have strict procedures that take ages to keep updating detracts from the work we are doing. Many individuals do a great deal of research and development whilst carrying out cases. I can see that future development will be massively stifled by ISO17025

Not very well

no.

Digital forensics is not clear cut as most people outside this arena believe. We have to find workarounds in problem solving and that means using third party tools etc. If drilled down by standard operating procedures this is going to bring us to a halt in what is an over worked environment already.

No, it's loosely fitting to the area and doesn't fit the requirement of adapting, as without doubt the digital forensic area will mutate further and further as new technologies are invented and embodied in society.

Yes, with effort and commitment

no. there are mant non standard methods used.

Yes but at great cost. ISO 17025 is only required because of poor management, that is organisational as well as staff and resources.

NO

No. I do not think it is a relevant standard for digital forensics at all

Yes, but not easily using the current guidelines. The practices appear to be designed for known specifics, in digital forensics we deal with an environment which can be changed depending on the variables in that environment which make it a lot harder to fit into the current ISO 17025 standards.

I have concerns about the validation and testing of forensic tools. Digital forensics is a fast paced industry with the continual need for new investigation tools, software versions and hardware. A requirement to consistently test all software and hardware used in conducting investigations will add significant overhead in terms of both cost and time. Such requirements are likely to cause a reluctance to upgrade software or use new and more appropriate tools due to the testing overheads. In my opinion this will increase turn around times, miss case relevant information not accessible to older tools and potentially provide inaccurate results when a new file format/version/OS is encountered which falls outside those encountered during the testing process.

According to the regulator yes, however at the pace technology moves ISO 17025 will be difficult to maintain without constant change and assessment.

If you bang a square peg with a large enough hammer, it will undoubtedly fit into virtually any hole.

yes, however digital forensic practices change depending on the circumstances/requirements unknown

No - alot of our work requires testing and some work can not be classed as 'standard'. Also on scene work has a number of variables which do not lend themselves to being restricted by SOPs.

No. In fact I am already observing double standards. A prime example, destination drives are forensically wiped before before use locally to stop cross contamination. However, the server has in excess of 50 jobs in one share, on one server.

Mostly, yes

no - technology constantly evolving so by time a methodology is validated and verified there is a high chance it will be obsolete in all but most basic process.

Not as currently defined.

No. I do not believe that ISO 17025 is a "good fit" for digital forensics. If there is to be an ISO standard for Digital Forensics then a new ISO standard should be drafted.

I think it is barely relevant.

No, it should be used at all, i'd like to use a standard that is designed for forensics. 17025 is square peg, round hole.

No. It barely applies to anything except the imaging process

Regardless, it will be made to fit, whether fit for purpose or not

Not really in it's current form. Not fit for purpose.

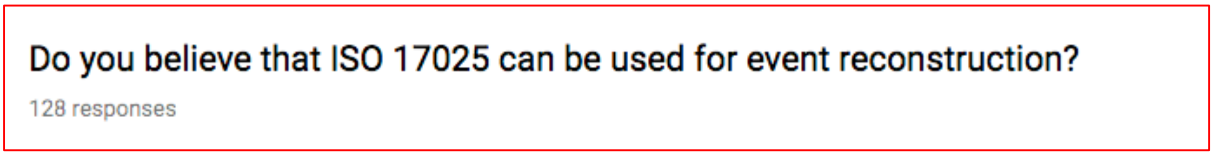
No. Section 5.4.5 of the standard outlines the requirement for the testing laboratory to perform validation on “non-standard methods, laboratory-designed/developed methods, standard methods used outside their intended scope, and amplifications and modifications of standard methods”. The pace of change of the field is such that this requirement would apply to almost any forensic investigation performed, as tools that have yet to be updated are applied to more recent (and untested) forms of the data under analysis.

depends on the optics

No.

No. I don't believe 17025 can be applied to digital forensics overall. The standards can show that our equipment is working the way it should be but forensics it forever evolving and changing. ISO is static and doesn't accept changes easily. It will work for things like DNA because they don't change that often.

No. because of report writing, defence work, and triage stage. All these stages need decision making by these who differ in knowledge and experience, and therefore not repeatable.
No, and in my view doesn't need to. I have an industy recognised professional qualification which I have kept renewed with CPD training. However I'm going to have to be re-compenency tested wasting more valuable casework time.
No,
Yes - to an extent.
No - I'd struggle to apply it to most of my cases involving computing since I don't do many run of the mill cases, most of the work I do is different on a case by case basis. As discussed above testing software and systems, testing if procedures have been adhered to, working on cases involving hacking, things like insider dealing etc. They are all too complex and different. If I followed a set procedure in my examination (obviously the basics are the same), I'd not find any evidence - computer forensics isn't all about technical knowledge and following a set path, you need a bit of creativity thrown into the mix to lead you on those tangents that actually find what you are looking for!
No, as there is a lot of events and scenarios that do fall out of scope and it would be impractical to account for everything, unlike wet forensics which are more or less far less complex
No
No, although we have been pushed down this route.
Not all. The arena of digital changes so quickly some technology will always fall out of scope before it can be decided if it should be brought into ISO 17025
NO
No. Mobile phone forensics is too volatile. Of course there needs to be best practice and documentation of the exam, qualified experienced staff etc, but you cannot test/validate/verify every single phone running all the different versions of O/S, user settings, hundreds of thousands of Apps that may or may not be installed and what version they are... the list goes on. And then not being allowed to update our software to the latest versions because they are not yet documented/validated is insane.
No, it should stop at data capture/extraction with the regulator or another entity developing a competency framework for digital forensics
No. I don't understand why or how ISO 17025 can have such a big impact on labs
No it cannot be done on site or when new unusual investigations occur.
not really appropriate for investigations (17020 is more appropriate)
No, it doesn't fit with all the processes.
No. Our particular work and the variety of processes and tools required is diverse. To test and validate all of these would require dedicated staff.
No. Imaging is possibly the only viable area for ISO 17025.
No, not at all
N/A
On paper yes, in reality there are areas where ISO accreditation is more of a box ticking exercise due to limitations in validation methodology and the complexity of digital devices. This complexity is not properly understood or taken into account by the standard.



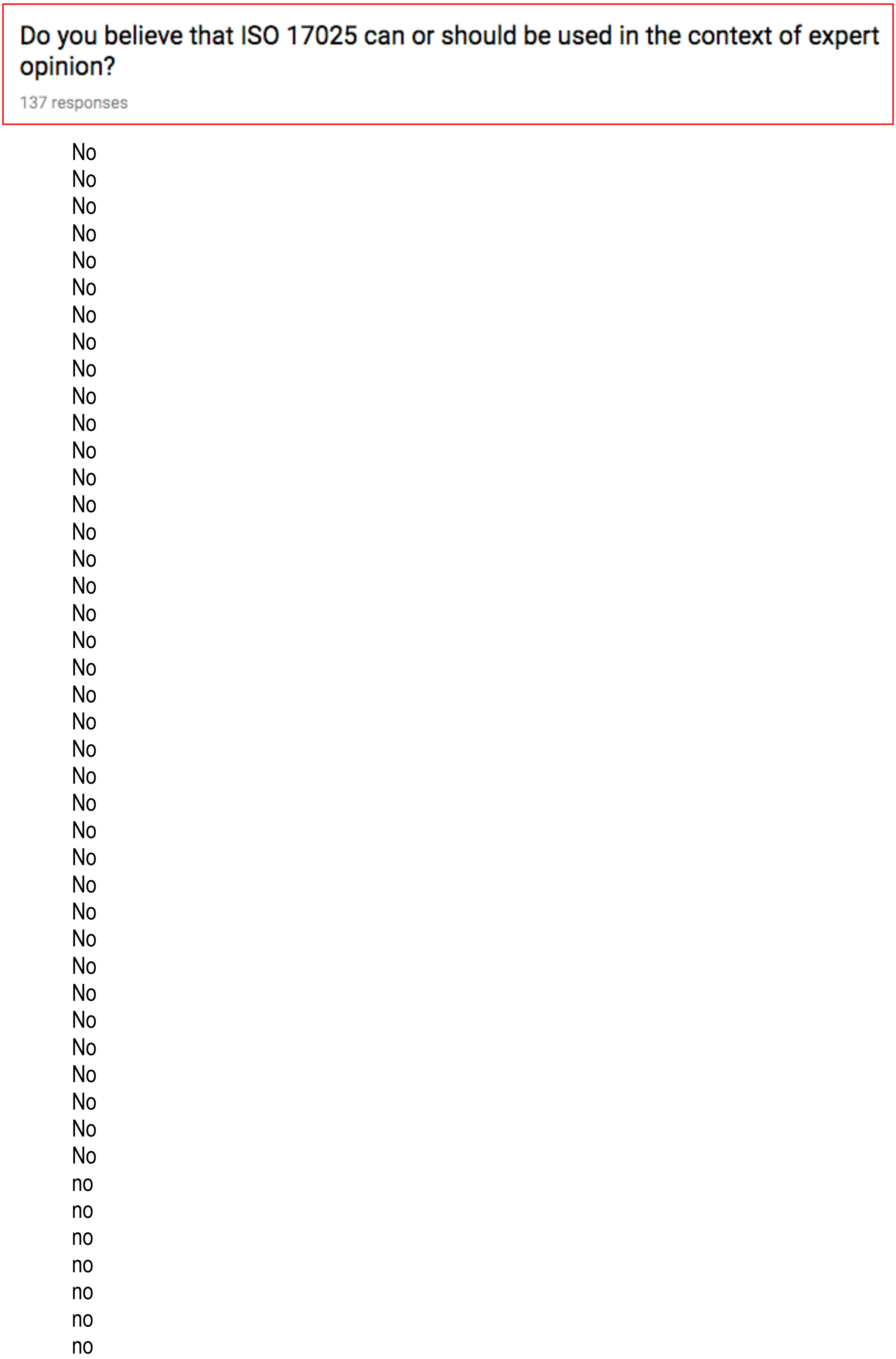
Do you believe that ISO 17025 can be used for event reconstruction?

128 responses

No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
no
no
no
no
no
no
no
NO
NO

NO
No.
No.
No.
Don't know
Don't know
Unknown.
Unknown.
unknown
unknown
yes
yes
Don't Know
Don't Know
Don't know.
Don't know.
I don't know.
I don't know.
N/A
N/A
Not sure.
Not sure.
?
?
u/k
u/k
Possibly.
It shouldn't be used
No idea. Sorry.
I suspect that some events may not fit the framework.
No. I previously wrote a response to the open consultation on validation and responded with an example where test sets are more complex than described in the proposed validation document. The document talked about not creating a single test set as the sample of how 'that' artefacts behaves in 'that' scenario, (which is correct). However it was far too simplistic in its approach. For example Yahoo brought out several versions of its messenger program in 2005 and in one change the same artefacts produced meant different things on these two versions. Of course both versions also allowed the user to make changes to what artefacts are created and could enable and disable these settings as often as they wanted. I've been the principal digital analyst in more than 700 criminal cases and worked on a very significant number of extremely high profile cases. I've had to carry out reconstruction 'test sets' on at least 50 occasions and on a number of different device types. I would not have been happy giving evidence in criminal courts and at the High Court, if I had followed the proposed approach in the validation document produced for that open consultation.
not entirely....mobile devices aren't a fully repeatable process due to such things as powering on logs, time and date etc
Do not know
Dont know
Leave it at imaging
Not essentially or exclusively.
Not to my understanding, no.

It can but again, will be expensive to implement.
Only for management review
Now that all depends on the case.
Not sure what you mean
Unknown
It would be quite difficult to validate all the processes.
I'm not sure what is meant by this.
N/K
It could be, depending on how the procedure relating to it is written.
unknown.
what?
We complete this already !!
No, categorically no.
No comment - Not applicable
no.
Don't understand the question
No more than currently provided by working in line with ACPO guidelines
Dont Know.
??
DK
No, but demonstrating you work within a standard helps assure my organisation we are competent to do so.
potentially
No. It is too restrictive.
Not known
No it is too rigid
dont really understand the question, however, if it means someone else recreating what has been done, then, yes.
Don't understand?
Unsure
No comment
No?
not in 100% of cases, so based on that, no.
Not sure how this would work?
This is not applicable to 17025, it is a quality management system to maintain processes. This question doesn't make sense
Not sure what you mean
Do not understand the question
Question is unclear
n/a
Not my area of expertise
Yes.
no comment
Not my area
Not sure what this means
Not sure, appears to rigid for such diverse scenarios
don't know
Yes



Do you believe that ISO 17025 can or should be used in the context of expert opinion?

137 responses

No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
no
no
no
no
no
no
no

no
no
no
no
no
no
Yes
Yes
Yes
Yes
Yes
No.
No.
No.
No.
yes
yes
yes
Don't know
Don't know
NO
NO
Yes.
Yes.
No
No
NO - an EXPERT is an expert
No. I don't believe that 17025 is relevant in any way to expert opinion or even expertise itself. It seems to me to have been produced for another purpose entirely, and it has no functional ability to assess or regulate expertise.
Only if there were some way of ensuring that all experts providing opinions are auditably playing by the same rules.
No. I think 17025 or another standard should require demonstration of competency in this area and qualifications should also factor. My concern is ISO 17025 costs so much there will be no money left for the prosecution to have analysts capable of giving expert opinion. There certainly won't be the defence experts available with the required expertise at the current rates permitted by legal aid.
Not sure
Not at this stage (acquisition)
Leave it at imaging
No. Fair enough for acquisitions but after that any work can be re-produced and let the courts decide cases as they do now.
unclear on question
No never! Systems are already in place - in a legal context - in respect of digital evidence.
Unknown
It can in showing that what they've extracted can be verified by processes, but if something were to change in the software or a version number changed, it could end up shafting the expert as it could show they aren't following ISO guidelines therefore how can their evidence be trusted. It essentially gives defense another line of attack, with minimum gain for experts as our evidence is already considered of a high standard in court...

I don't believe being ISO17025 accredited makes one an expert, so NO.

Yes as an initial tenant to build an argument for a case

no because ISO does not validate a person, just that they can follow instructions - sausage factory forensics

No, opinions are subjective, ISO17025 cannot test is the opinion meets some arbitrary "quality measurement". A battery may be "12V or above" to met a standard and opinion cannot be quantitatively measured.

Yes and it is already being asked at Court by Defence Counsel

I think it can add an extra layer of integrity to our practices.

Possibly

No. If any was to be used, 27037 should be used. Standard adoption should not be able to indicate validity of evidence - 17025 adoption does not mean that every exhibit has been analysed to the same standards, human error still present.

Probably but it's still unhelpful

I almost never give expert opinion and am not sure I wil have it in scope at first. However it can and should be used - although it is technically ILAC G19 which sets the standard.

No. In the event of failing to achieve ISO, we expect to continue as normal and challenge Defence Experts to show where we have gone wrong.

No reason why it shouldn't be used for expert opinion, however, not appropriate for research and testing etc.

yse

We relied upon ACPO before ISO17025, all ISO does is create additional overhead with arguably not much benefit.

Not really

Don't Know

We attend court as a professional witness and not an expert and really shouldn't be giving evidence of opinions. I believe that 17025 should not be used as my professional details are clearly given and have never been challenged

No, because if an 'expert' starts stipulating ISO 17025 it will be quite obvious that they themselves do not understand what ISO 17025 is and how bad it has affected the digital forensic world and consequently, quality of the evidence has been diminished with unnecessary red tape.

I do not believe that it is applicable to the context of expert opinion. ISO 17025 attempts to ensure that all reasonable efforts have been made so that the expert opinion can be competently formed and/or that the integrity of evidential output is maximised.

Standardised responses should be key, expert opinions should be based on factors which should be measurable. As such they could be subject to a process such as ISO 17025.

Dont Know

It can be used, but I don't think it should as it may take emphasis away from the physical evidence within a case.

DK

Yes, this is part of the opinions and interpretations of the standard

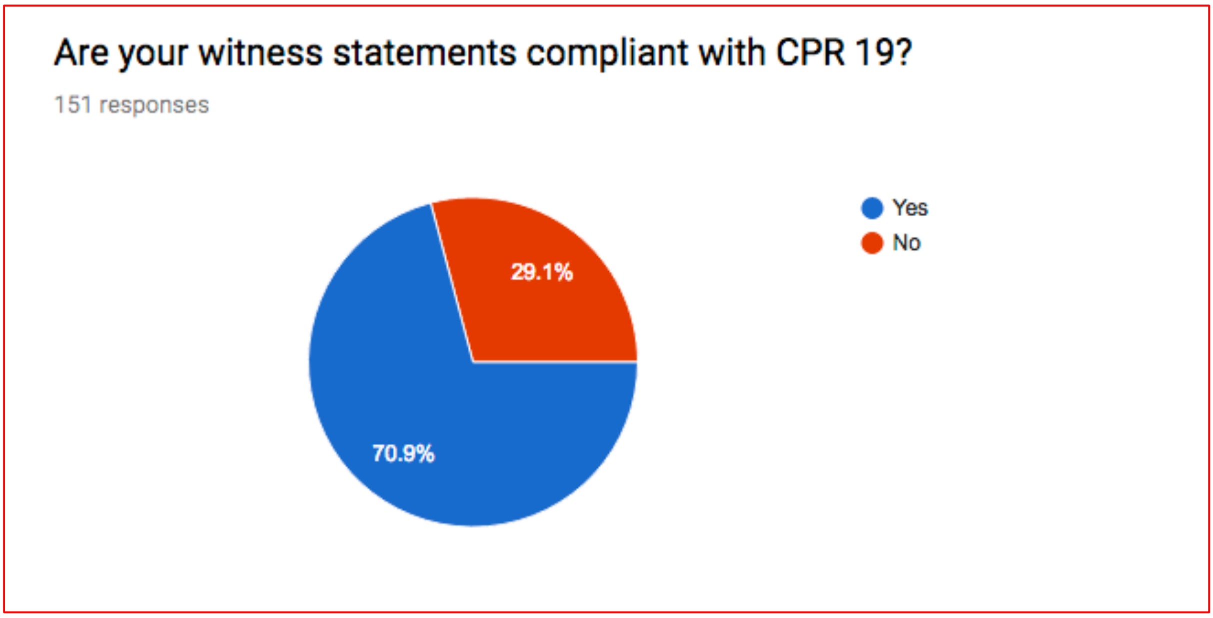
ISO17025 does not prevent an 'Expert' doing poor work or blatantly lying on the stand. A recent case we defended not only saw the Expert, from an ISO accredited commercial company, LIE about the issues with the phone, LIE about why it was examined but he even LIED and said HE examined it - when it was someone from another country. Conclusion - ISO accreditation does not guarantee reliable Expert testimony.

Np

I haven't considered this.

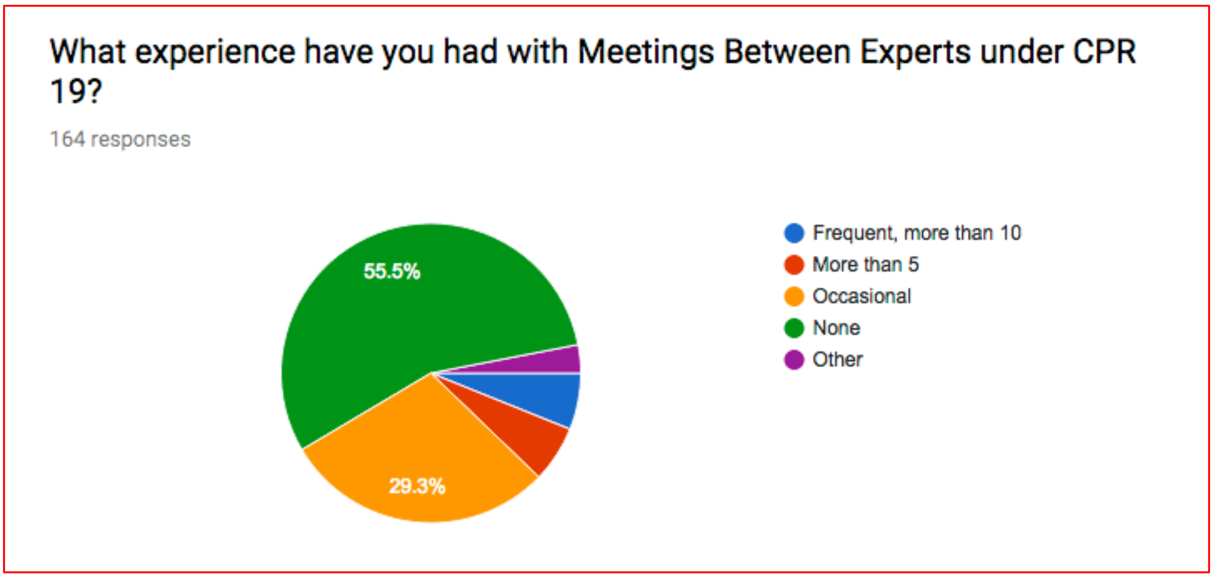
Not within Digital Forensics

No. ISO 17025 is so tied to processes that it doesn't seem to allow for the use
No but methods should be validated as fit for purpose
AFAIK it can't, UKAS do not accredit opinion.
In this context yes, because it will demonstrate that the experts expertise is tested and current.
No it is a cobbled together standard
Ambiguous question
n.c.
Can be used.
If by that you mean can/should following the certified iso 17025 procedures be questioned at court then yes, but again, because of ACPO, if they haven't been followed then its documented as to why they haven't been followed/reproduced.
No, this is the whole point. Am I likely to not get called to Court to give evidence just because my organisation is 17025 accrediated ? - highly unlikely. I feel the Judiciary will pay little heed to this, and it will certainly not change the rules of evidence in Court.
Not sure. Although if this a required standard then yes it should be used.
No, the FSR codes covers this though
No. It will stifle the ability to examine computers fully and be able to provide full unrestricted opinions.
Possibily, however I do not fully understand why it has been implemented. We we still be required to go court and explain the results - has no meaning or relevant as the data/procedure will need examining, regardless if it is accredited.
Where possible yes, but it should not be the be all and end all.
In the context of digital forensics, no. The expert opinion is subjective, as is the opinion of the "independent" UK as auditors. Impossible to achieve consistency. Must look at industry-wide competency framework to stand along side 17025 for more advanced analysis
n/a
Not sure. Procedures are one thing, but an expert has to be able to interpret and convey information for which tools may not exist.
sometimes
Not sure.
No, I am standing in the box, not anyone else. I have had the training, experience, carried out my own verification and its my job on the line.
No, its not "validateable"
Not sure
From what I have seen 17025 has a proper place for laboratory tools and practices. It appears to me not the correct vehicle for dealing with the more flexible approach taken for expert interpretation, which is more based around the individual's interests and experience, which is different for each of us
Maybe
In its present form - no.



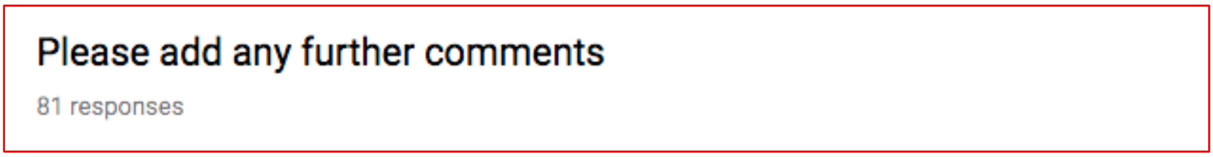
Are your witness statements compliant with CPR 19?

151 responses



What experience have you had with Meetings Between Experts under CPR 19?

164 responses



Please add any further comments

81 responses

None

None

ISO17025 does not consider non standard investigative problems

Although we have worked on well in excess of 500 criminal investigations since we started in 2002 (including Operation Ore and other National and International investigations for law-enforcement), the requirement to be ISO27001 certified is just too expensive for us, in time. We will remove ourselves from criminal prosecution work and focus on the areas where profit can still be made. I note that if we had found ISO27001 to be some kind of an assurance of quality, we would have considered spending time on getting certified (we are already compliant IMHO, probably actually working to higher standards) but the reports we have received from other experts with the certification have been AWFUL; literally pages of irrelevant material stating 'in compliance with ISO27001 standards we have...' etc. More pages of this than evidence - what a waste of time and effort.

Due to the introduction of this ISO, as a company we are closing and thus removing a valuable resource from Law Enforcement in the UK that has spent 19 years building our knowledge and expertise in niche fraud investigations. As a small company [2 people] we can not afford the accreditation and feel the introduction of this ISO has effectively created a monopoly for the few but large forensic companies that provide a sub-standard service to LE

Hope the above is useful in slaying this rather pointless monster.

I don't believe a need for ISO17025 in digital forensics has been justified and I am surprised that the cost of it has not been considered. I think it will mean less money for training, software, equipment and staff numbers. Ultimately less qualified staff, with less equipment, with a smaller range of software tools, will spend less time on each case.

ISO is quite possibly the most damaging thing to be associated with Digital Forensics. The nature of our job negates the need for the buricracy associated with ISO

I hope the regulator listens as its impossible to achieve and maintain. Also since she has no statutory powers police forces should be refusing to do it

so far only working towards imaging and extraction

ISO can not be applied to digital forensics. Its a total waste of time and money

Iso 17025 is a necessary benchmark that digital forensics requires but as a practitioner with 20yrs experience and a Managing Director of a company who went through the pain and extortionater cost of ISO 17025 it should be left at the imaging stage!!

The bottom line is I don't know what the problem is that the introduction of ISO 17025 is looking to solve. To the best of my knowledge there isn't, and never has been, an issue with the quality of digital evidence produced for use in Court. This is not 'wet' forensics and there are minimal risks of cross contamination. Changes to evidence are easily and clearly demonstrable through changes to hash values and therefore any changes have to be accounted for and we are used to doing this at Court if required.

If pushed, this so called 'standard' could have severe implications for my business. I am focused mostly on private markets and small private cases for SME's or private individuals. If my company, or others like me are forced out of business, then that could exclude certain sections of the general public & business having access to Digital Forensic Services. [mostly on grounds of cost]. The ironic part of this is the fact that if any of my cases were done by a larger company or law enforcement officer, [as I have discussed with several former colleagues] - as long as we are compliant in the legal aspect of obtaining, verifying and submitting digital evidence in Criminal or Civil cases, then we have both worked to a same standard and will both achieve the same results! When you take this analogy, then one has to question a need for a stringent ISO compliance that will force itself on ALL practitioners.

ISO is not compatible with data forensics today. Causes more work than needed and not flexible. Is slowing down the forensic process.

I came into forensics a year before ISO 17025 came into place and what I've seen is a real change of culture in our workplace, from what is supposed to be investigative forensics (finding one piece of evidence leading to another, like a chain reaction) into following ISO standards where we can no longer chase down the chain and instead stop where our standard operating procedures tell us to stop, it basically shackles us. There is a procedure in our ISO manual to say that we can do "infrequently used techniques" which would cater for this type of chasing, but you need to know what exactly it is you are aiming to obtain, plus it has to be approved by a bunch of working groups and management meaning by the time you actually want to do something like this, it becomes such a hassle that it slows the whole forensic process down. What I have noticed though is having everything asset registered means we have a great idea of where kit is, and maybe that is something that should've been done well before ISO but being forced to do so under ISO has been something of a help, albeit a very tough exercise to tag every single bit of kit we have... The real issue I find with ISO comes down to the deadline though, which is supposed to be October 2017. I simply don't see many, if any forces reaching this deadline and I cannot speak for the private sector but looking at what has happened to Sytech recently (losing part of their accredition) shows that even those who were well prepared are being shafted too. If the forensic regulator is serious about closing down units before they meet ISO 17025, I can see a crisis that's almost imminent.

ISO has been deemed necessary, and is being forced upon law enforcement. It is an unnecessary and expensive implementation which has been put in place to fall in line with other forensic departments' implementation of ISO 17025. I do not believe ISO 17025 is compatible with digital forensics for many reasons. The two most important being cost to implement and maintain and it doesn't cater for when things don't go to plan. We still have to cater for the unforseen.

17025 is best suited to a discipline where there a few processes, that rarely change and a subject area that is not highly dynamic. In terms of items to be examined and methods used. FSR and ISO17025 like the failed CRFP before it may have laudable intentions but they cannot achieve what they set out to do.

17025 has been a revelation to Digital Forensics.

A dedicated standard needs to be written rather than try and shoehorn DF in 17025 which was written for black/white lab procedures. It simply does not fit into the digital world.

In the realms of my organization, the implementation of 17025 has been borderline crippling to productivity

I am not a supporter of ISO accreditation for use in digital forensics. The monetary cost is prohibitive and particularly so at a time when force budgets are being severely constrained. Overworked staff are being asked to take on even more work and responsibilities and I know quite literally no practitioners who believe this is a good idea. Over the next few years ISO accreditation will in all probability be quite literally a get out of jail free card to some of the most reprehensible and dangerous individuals in this country. There will be instances of society's most vulnerable people (who we are supposed to be protecting) being put at risk of great harm due to ISO 17025 compliance and the technicalities that it will allow for in court. In essence technology is advancing in our area of expertise at a great rate. Budgets are being constrained and overworked and stressed staff currently struggle with backlogs of work sometimes over a year long due to a rise in offences and offenders being identified. Under these circumstances we should be looking at how to make the system more efficient, not attempting to enforce what at times seems like needless bureaucracy which will only make most organisation's digital forensic capabilities a great deal less efficient.

I believe the standard is not fit for purpose and should have had a bespoke and more appropriate standard developed. As each organisation has had to develop its own procedures based on their own interpretations of the standard, I see little opportunity for standardisation of results across the industry.

This is a dreadful standard and doesn't/can't apply to digital

ISO17025 is not relevant to forensics, 27037 is Digital Forensic standards which is perfect fit for all labs to adopt.

We're currently considering ISO 17025 but holding off due to the time/cost requirements and seeing what happens with it. There have been lots of these things in the past like the CRFP which get pushed very heavily but always meet resistance due to the excessive time/cost and poor applicability to digital forensics processes and appear to always be based on large scale automated forensics fields like DNA where the number of tools/processes are far fewer and rarely change.

Working toward 17025 has made me want to leave computer forensic examinations. I believe it stifles innovation and makes examiners think twice about using methods that they know will take an age to validate and write up. I have been involved in forensics for nearly 10 years and I now want to leave. The cost is horrendous and the ONLY people who benefit, from what I can see is UKAS.

As I mentioned above I was unconvinced by ISO17025 as a standard for digital fornesics at first, but I decided that it was probably going to happen and implemented a system from 2011, which is now fairly mature, although there were a few "big ticket" items involving business continuity. There could be a better standard for digital but, with the codes and annexes, it does work. My experience of UKAS is that they are being broadly sensible in their approach to validation and competency. Basically most of us (including me, and I've done quite a lot) have left things too late - but we can't say hat he Regulator hasn't been extremely clear in saying that the deadline will not move again and that she wants statutory powers.

There is nothing wrong with using ISO 17025 for the most part for most examinations and overall it has improved standards and increased quality in our environment. However it cannot be employed in all circumstances and these need to be written in as exceptions in SOPs to avoid non-conformances. The cost and time impacts are very high for the marginal gain in quality that could be achieved through less intrusive methods.

The cost of 17025 (accreditation and on-going) is unreasonable and only seems to benefit UKAS. The ISO itself is not a good fit with any aspects of digital forensics and the Forensic Science Regulator has given very little if any thought to bodies outside of the UK Police Forces.

ISO17025 is a disaster for computer forensics and future innovation in this field

For standard jobs there is no reason why 17025 can't work. Where jobs require further specialist work is where the problem is. This is OK where we have the cover of 'infrequently used method', however, we have been told that if the method is used by the unit more than 3 times in any year then it is not infrequent (so a procedure should be written)! Arguably, this could be used as a back door to get untrained staff to do the work as they simply 'follow the procedure' which greatly increases the risk of evidence being missed and poor quality work.

With standard procedures and standardized builds (software and hardware) innovation and progress will not happen and will be incredibly slow. Where it is tried it will be stifled with bureaucracy (change requests, authorization, everyone implementing the change requested) even for something simple, often times cases don't have the luxury of this time delay. ISO 17025 seems better suited to chemical labs, DNA and fingerprints where an examination is possibly a couple of procedures that each may take 5 minutes. Not a long list of procedures that may take several weeks.

The overhead in both time and effort on conforming to ISO17025 seems to be excessive. ISO17025 seems to want to lock down the way forensics is conducted on the ever changing world of digital technology. The range of devices mean that a range of processes is required to successfully analyse these items. This cannot be tied down to a set of strict procedures. The amount of time taken to comply with ISO17025 can quite easily take away the time available to complete digital forensic investigations at high quality.

I firmly believe there should be standards nationally and this should of been led by a group of experts to write this standards for the whole of the Police Forces. Any standards should be done Generically so there is areas to manoeuvre within the standards. For example there are different Forensic software being used. One may recognise one file system whilst another wont. 17025 should be watered down, but if brutally honest set guidelines could of be easier that going down a lab accreditation route. I believe that collectively we should fight this accreditation and come up with alternatives - But is it too far down the road now.

Who ever thought green lighting ISO 17025 in the FSR was, in my opinion, having a really bad day.

significant amount of staff hours taken up with ISO17025. not sure if a different set of standards would have been better for digital forensics.

Typical of government project, decisions made with a "one size fits all" mentality. 17025 is a good standard but not for the fast moving digital world. A different standard should have been created. Any well run digital unit/company does not need 17025, the trouble is there are lots that are not, and they will benefit from it.

I don't know what CPR 19 is so no idea whether witness statements are compliant or not.

None to add

I spend all available time carrying out casework. I cannot make a profit if I need to dedicate my time to producing quality manuals etc. I would need to employ additional help and the current legal aid rates do not provide sufficient headroom to do this. Effectively ISO17025 puts me out of business.

N/A

A system well intentioned however not practical for digital forensic work in its current guise.

Personally, whilst my force is fully onboard with ISO compliance, I find it to be clunky, and needlessly complicated to the point where updating my software and hardware becomes a thing of dread. "Shall we update to the latest version of Encase?" "No . . .we don't have a week to complete verification"

ISO 17025 was written for wet forensics - 'shoe horning' it into digital does not make sense, and the whole 'customer' concept doesn't quite sit in Law Enforcement.

Overall I can see this being useful. However I feel it has been rushed through. I believe it is badly thought out with constant contradictions. EG, each forensic workstation is validated yearly on standardised images for preview purposed, they all return the same hash values. Yet we are only allowed to acquire on specific workstations which have only approved software installed and are locked down. These workstations also return the same has values. The amount of time wasted on document reviews is overwhelming, we can get 2-20 updated documents a week. These maybe a new doc, or a spelling mistake corrected and we are supposed to review them again, often written in management speak with 6 pages of pre-amble. If validated software gets a minor update, the release notes are read and based on minimal changes, it is automatically approved. In other words, it feels like a random 3rd party company is trusted more than us practitioners, as we have to justify and verify everything we do.

This attempt to frustrate the FSRs requirements by the F3 is too little and too late, sorry but this has been coming for the last 5 years.

SFR/1 does not detail file locations (in cases with IIOC etc) and this information is essential to a defence examiner when analysing the prosecution evidence.

17025 is a great idea poorly executed - we are a standards oriented organisation that is hugely frustrated by the inappropriateness of the current implementation. 3/10. See me after class!

ISO 17025 may be fine for large laboratories doing DNA work for the Prosecution. It is not proportionate to much digital work. Any attempt to extend it to expert opinion is misguided or worse, reflecting a misunderstanding of the body of expert practitioners. In particular it will damage justice by forcing Defence work into the hands of large firms which specialise in Prosecution work.

ISO 17025 will basically stop any organization from using the right tool for the job, rather encouraging them to make the accredited tool fit. This will cause loss of evidence and all the implications that come from the CJS

Please, please review the requirements of ISO17025 and reassess the value and relevance for Digital Forensics work as the more in depth review made, the more irrelevant the standard is.

ISO 17025 is not fit for purpose with Digital Forensics. If it is supposed to be an industry standard, how is it that every force and practitioner will still have different processes and standards. UKAS should be much more helpful and advisory, but do not appear to know exactly what they are doing either. ISO 17025 does not assist investigations in any way, if anything it currently is a hindrance and is slowing down case processing times.

The community already regulates itself via the court process.

Not enough is known about ISO17025 by myself apart from the restrictions it is putting on myself and colleagues to continue to offer a good service by restricting my ability to conduct work. I am in agreement with standardising services and procedures and believe this definitely needs to be done however the way it is being implemented I think is not the right way. It is causing major stress levels within the unit and it is becoming more and more difficult to do our jobs.

The collective feeling from the lab is that ISO will provide the defence more potential issues to raise in our evidence (a proverbial 'stick to beat us with'). ISO certainly creates a lot more bureaucracy including the constant calibration, the forever encroaching standards, the need for auditablilty at every stage including that of deleted data, the changing of documents, raising of non-conformance etc... this in turn takes a lot of time, a dedicated practitioner who could be better placed completing casework (as fundamentally that's what the police force is there to do) and over complicating very simple procedures. As example, raising a non-conformance is a long-winded process for what could be a very trivial issue, which could be more efficiently dealt with by just explaining the error to the individual who made it. We feel that being forced to work by iso standard regulations, demean and belittle the work that we have previously produced over the years. The standard of work before ISO regs was clearly up to standard as it helped OIC and CPS investigate/charge a suspect beforehand (which primarily is what my job is) so why do we need it now? ISO is relevant to 'wet forensics' which rarely change procedures over time, whereas it is not suited a digital environment which is more investigative based (hence it shouldn't be under the 'forensic' title/department) and forever changing at an increasing speed because of new technologies. A classic example as to why ISO regs increase the time we need to do simple procedures is that of investigating a USB stick. it takes longer to complete all the needed paperwork due to all the duplications and constant double checking that all stages in the SOPS are complete so we don't get questioned if it goes to court, than it does to actually examine the exhibit

My greatest worry is cost, I feel the level of scrutiny that accrediation involves will result in a large percentage of everyone's time being taken up with evidencing processes and proceedures. This will lead to paralysis by analysis.

ISO17025 should not be forces on forensic labs. A new standard to cover the testing of tools should be implemented and vendors of tools should be responsible for certifying their products.

No further comment

Some of the questions do not make full sense to me.

I have personally seen a large decline in quality of work in the past 2 years in both computing and cell site analysis including from firms/police forces working to ISO 17025. In some cases, I have noted serious errors and/or large amounts of missed evidence. Reports I mostly see in computing are often now just lists of facts, no tying the case together and often missing very important evidence which would make a strong complete case. I am not sure if this is due to ISO 17025 or lack of funding, or perhaps both. However, it will mean ultimately a huge amount of wasted money from other 'pots' when costs involving lawyers and court are taken into account. Cell site analysis conducted by the police in-house in my experience is generally very poor. Facts can be very misleading if appropriate knowledge and quantification are not provided. Cell site analysis is and always will be an expert opinion based area only.

I work at an airport and mainly perform a triage/intelligence gathering function. Whilst I understand that triage/intelligence can lead to evidence and as such acquisitions should be performed to the expected standard, I feel that ISO 17025 is overkill with regards to costs, training and procedures.

ISO 17025 has taken processes we used to be able to do quickly and competently and added a significant bureaucratic overhead that means we are much more likely to make an admin related mistake. These processes also now take far longer due to the admin overhead. The application of wet forensics principles to digital forensics case processing is not a good fit. Too often the assessors have told us we are doing it wrong without being able to come up with an alternative. I agree with the need for standards but applying a bunch of standards that derived from wet forensics is not the way to go about it. Do it properly or don't do it at all and let the court decide if it was done properly.

I understand that 17025 is there to increase standards, but it is very bureaucratic, time consuming and expensive, the standard is not totally suitable for digital forensics and should have a seperate standard.

I agree that processes need to be implemented but ISO17025 is making the process far to complicated and long winded. The amount of data I process is considerable and the ISO process will compound the time constraints place on us by courts to meet disclosure deadlines. The ISO accreditation process is like a square peg into a round hole, far to expensive and . The people auditing and issuing accreditation are to removed from the day to day realities of Digital Forensics. Will defence experts who do not have ISO accreditation have their evidence refused in court. IF not why should Law enforcement have to abide by ISO. ISO feels like a Quango emptying public coffers of tax payers hard earned money.

I am finding the iso preparation to be overly wordy at the moment and hope that when it is place it will make sense and be worthwhile. I think iso standards are necessary in forensics but at the moment appears to be made overly complicated where everything seems to have a procedure except the examination process which should have been decided at the start.

Experience of dealing with multiple forces and defence companies shows most still misunderstand requirements for 17025. It is cost prohibitive for small firms and individuals and regulator has failed in her promise to assist in this area in any meaningful way. Consultations of FSR with the industry have been far too minimal and closed door, which is shown in her militant approach and misunderstanding of many aspects of the industry, as well as a blind ability to continue to believe that accreditation alone will deliver high standards in forensic science. In this she is wrong.

I think it is a sledge hammer looking for a walnut to crack.

I have only taken over the department in the last 7 months and expected to achieve this standard by October. The amount of literature on this matter alone has taken weeks to read. The CCTV scope annex released is vague and subjective. To complete this work on top of trying to run a busy operational department is proving extremely difficult and frustrating. I appreciate a need to improve quality but are there no better and more cost effective ways to achieve this?

WHilst there are many things wrong with it, validation is one of the biggest things that strikes me. Technology changes every day and its impossible to have a validated method implemented for every scenario. Why test a handful of things, when the scenario's tested may not even apply to the case. Furthermore, the validation should have been attempted by one central organisation and rolled out (similar to NIST). Everyone is duplicating each others work and wasting time, money, resources individually when it could be done nationally.

Even with approx. 80 people working within our department we only have 1 quality manager who has taken on the new role and still trying to understand what is actually required. Even the most technical members of the team are struggling to understand the process for tool testing and validation. Every department seems to be doing it differently based on their interpretations.

This feels very much as if the FSR may lack DF knowledge and rely on a selected set of advisers who will say anything (even if not practical) to remain at the table. When a practitioner has 30 on-going cases, we simply do not have the time to send them on ISO training or to even get involved.

The standard is not tailored for Digital Forensics - our expert area is ever evolving and does the standard is too rigid to enable practitioners to experiment and work inventively.

As far as I can see, ISO was decided for all forensic sciences without any actual thought on how it would apply to each one. For the most part, what Digital 'labs' do is investigation and I cannot find a single example of where ISO 17025 has been applied to ANY type of investigation, probably with very good reason. This standard has already started limiting what companies will do, with one of our outsource providers informing us that they cannot image surface tablets as they can't use FTK and a writeblocker to do it. This has been echoed by a number of police forces who are no longer looking at newer and better ways to do tasks as that will include a heavy amount of paperwork, cost and time. All this at a time where forces are already stretched thinly. Nothing I have seen from the ISO process has given any indication that the "validated" processes are in any way validated. They often consist of small number of devices (especially in phones) with very limited scope and this then covers for extraction of all phones, with any app type and OS, regardless. Having read 3 or 4 different validation plans for phones from different forces/private companies I can honestly say none are worth the paper they are written on and have been done to 'tick a box'. The competency side of the ISO is a nightmare, as increasing the number of techniques adds a burden to competency check all individuals using these techniques. The FSR guidelines are even more problematic here as ISO would allow us to call people competent based on experience and qualifications, however the guidelines call for regular reviews. All in all, applying this ISO to Digital Investigations was a badly thought out idea which is now being forced through with no common sense or actual thought based on someone ideological idea of how something should work without any actual knowledge of the area

Imposing ISO17025 on the DF industry in this coutry has caused huge pressures and costs for nothing. If the FSR is truly concerned with the quality of evidence produced by HTCUs then there are other routes than this nonense. £21000 for an initial assessment is a truly incredible amount of money for what amounts to a coin toss.

The team is working with other law enforcement agencies to ensure that as far as possible that standards and procedures are ISO17025 compliant without actually seeking accreditation.

It is good to have guidelines and processes to follow in forensic departments but ISO is far too in depth and is unnecessary. It is impossible to constantly keep validating every single version of all the software used, the actual forensic work would never get done. Too many issues to raise in this questionnaire. It is obvious that ISO is trying to be introduced by people who have absolutely no idea how a forensic department is run.

I am personally more than comfortable with being assessed or judged on my capabilities. 17025 does not appear to be the vehicle for resolving that.

do senior management know the importants of ISO?, I think not

IS0 17025 I agree fits well with some areas of Forensic Science. However, it is not feasible for Digital Forensics as we don't have a standard way to examine devices. It depends on the make of the device, OS version which is running, encryption, type of case and much more.

No comment