



Competence in digital forensics

Graeme Horsman^{a,*}, Andrew Dodd^b

^a Cranfield University, College Rd, Cranfield, Wharley End, Bedford, MK43 0AL, UK

^b ADAS Ltd, UK

ARTICLE INFO

Keywords:

Digital forensics
Competence
Digital evidence
Practitioner
ISO/IEC 17025:2017

ABSTRACT

Those practising in the field of digital forensics must be competent to conduct the work they carry out, and such competence must also be evidenced and assessed. Those seeking to demonstrate staff competence must consider what tasks and roles it is being sought for, how it is achieved, what is an acceptable level of performance for a task, and how to evidence and assess any claimed competence. This work intends to explore the multifaceted nature of competence within the field of digital forensics, examining how it is developed, assessed, and maintained in an era characterised by continuous technological advancement. Discussions are also linked to the requirements defined in the accreditation framework ISO/IEC 17025:2017 which governs the digital forensic landscape in England and Wales. We hope to contribute to the ongoing discourse on elevating standards and fostering excellence in the science of digital forensics.

1. Introduction

The importance of digital evidence to law enforcement inquiries has been emphasised in recent years (Muir and Walcott, 2021; Interpol, 2024) due in part to it being present within many of the incidents that require police investigation (National Police Chiefs' Council, 2020a; College of Policing, 2024a), and it's potential to describe the conduct of relevant parties involved. As a result, the demand for digital forensic (DF) device examination has, and continues to increase (His Majesty's Inspectorate of Constabulary and Fire and Rescue Services, 2022). With law enforcement and criminal justice systems maintaining their reliance upon the services of DF professionals, there is an expectation that the work that is produced and supplied by them is of an appropriate standard so that it can be relied upon when used to inform future investigative and legal decision making (The European Network of Forensic Science Institutes, 2011; Losavio et al., 2016; Doyle, 2020). To achieve this level of work requires those that are involved in, or performing any forensic tasks to be competent to conduct the work they are required to do. Whilst this is an obvious requirement, the task of understanding, achieving and evidencing competence is not always straightforward.

It is first necessary to state that being competent does not guarantee acceptable performance for a given role or task as it is reasonable to assume that human error can always occur. However, the presence of competence should increase the likelihood of it being carried out to an acceptable level. Fundamentally, being competent means being able to

perform a certain job well (Stockwell Safety, n.d) and having 'the ability to apply knowledge and skills to produce a required outcome' (Trinder, 2008). As a result, acceptable performance for a role/task deemed within someone's scope of competence is more likely to be witnessed than if it were performed by someone who is not competent to undertake work of that type. Hence, why competence is so important within the forensic science domain.

The concept of competence might arguably be considered deceptively simple (Le Deist and Winterton, 2005), particularly when being considered and evaluated in fields of work where many operational complexities exist; forensic science being one of these domains. With a particular focus on the sub-field of DF, competence forms a cornerstone for good practice and quality management, but the requirements surrounding it, and how it is evidenced may differ between jurisdictions. In environments operating under accreditation frameworks, as seen in England and Wales where the forensic landscape is governed by ISO/IEC 17025:2017, competence requisites are formalised, and they must be met and evidenced if accreditation is to be sought. In non-accreditation driven landscapes, competency requirements and approaches to evidencing competence may differ, for example, ISO 17025 in Northern Ireland and Scotland is voluntary matter for the organisations involved. In England and Wales it is a compulsory requirement for DF service providers where activities are described in the FSR Code under threat of legal action. Competence is also referenced in many of the overarching guidelines that are in circulation. For example and whilst historic in

* Corresponding author.

E-mail addresses: graeme.horsman@cranfield.ac.uk (G. Horsman), andy.dodd@adas-ltd.com (A. Dodd).

<https://doi.org/10.1016/j.fsidi.2024.301840>

Received 17 July 2024; Received in revised form 1 October 2024; Accepted 1 October 2024

Available online 11 October 2024

2666-2817/© 2024 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

nature, the widely acknowledged ACPO principles for digital evidence directly references the need for competence in their second principle, and throughout their guidance documentation ([Association of Chief Police Officers, 2011](#)) (*note - ACPO no longer exists and whilst the original principles are still valid and excellent guidelines, they are only guidelines and have now been superseded by the FSR Code, having not been updated for over a decade*). In more recent times, the Forensics Science Regulator's (2023) Code of Practice at Section 28 stresses the requirement for competence and details what is required of laboratories to show their staff maintain it.

The importance of professionals possessing competence in the field of DF cannot be understated but achieving it can pose a series of challenges. Those seeking to demonstrate staff competence must consider what tasks it is being sought for, how it is achieved, what is an acceptable level of performance for a task, and how to evidence and assess any claimed competence. This work intends to explore the multifaceted nature of competence within the field of DF, examining how it is developed, assessed, and maintained in an era characterised by continuous technological advancement. We hope to contribute to the ongoing discourse on elevating standards and fostering excellence in the science of DF.

2. Competence and DF

Competence is a global concept in the sense that all those in DF should be competent in regard to the activities they conduct, wherever in the world they are practising; the same is true for almost all disciplines. However, as noted above in section 1, competence requirements may differ both jurisdictionally, and in accredited and non-accredited environments. This work will try to give a holistic insight into the meaning and implications of competence in all cases, whilst providing focused examples. Discussions will naturally gravitate towards the positions set out in the international standard for testing and calibration laboratories - ISO/IEC 17025:2017 given the impact and role it is playing within the domain of DF. [UKAS \(2024a\)](#) is the national accreditation body and assessor of ISO/IEC 17025:2017 in DF laboratories in England and Wales. The International Laboratory Accreditation Cooperation (ILAC) (2022) notes that accreditation frameworks and adherence to them helps to lower the risks posed to both any accredited organisations' customers and to the accredited organisation themselves, as it demonstrates that they are competent to conduct the work that falls within their accreditation scope. Where possible, a generalised discussion of competence will also be offered.

The National Digital Forensics Strategy ([National Police Chiefs' Council, 2020b](#)) in England and Wales emphasises the need to professionalise DF science roles, improve career opportunities and ensure that a culture of continuous learning, supported by a national competency framework and training operations is created. The field is both wide and diverse in nature in regard to the numerous forensic techniques used across the vast range of available devices, and deep and complex in regard to the elements faced in many investigations. The increasing complexity within digital examinations is presenting more challenges with a growing number of device types holding potential investigative opportunities that must be identified and understood, the use of data protection and obfuscation techniques, ever expanding varieties and data-formats, more information being stored in the cloud, and the rapid growth of the 'Internet of Things' ([National Police Chiefs' Council, 2020b](#)). Practitioners may also face investigating crimes that range from the possession, creation or distribution of child sexual abuse material, malware, grooming, illegal online behaviours, to the extraction and interpretation of information that may help law enforcement to understand any relevant parties physical course of conduct (for example, stalking and location information). As digital crimes become increasingly sophisticated, there is a rising demand for DF experts who possess a 'high level of competency' ([National Police Chiefs' Council, 2020b](#)).

[Rose \(2021\)](#) notes that the term 'competence' may be utilised

frequently within workplaces without it being fully understood. Discussions surrounding competence and any decision making relating to it can be both complex and challenging as not everyone considers and interprets this concept in the same way ([Hoffmann, 1999](#); [Le Deist and Winterton, 2005](#); [Vitello et al., 2021](#)). Further, we have already noted that domestic and international perspectives on how it should be assessed and evidenced within forensic organisations may differ in terms of approaches, guidance and requirements.

Starting generally, the [Cambridge Dictionary \(2024\)](#) defines competence as 'the ability to do something well', or 'effectively' ([Collins, 2024](#)), with a competent individual being in 'possession of required skill, knowledge, qualification, or capacity' ([Dictionary.com, 2024](#)). The [Health and Safety Executive \(n.d.\)](#) expands, stating 'competence can be described as the combination of training, skills, experience and knowledge that a person has and their ability to apply them to perform a task safely. Other factors, such as attitude and physical ability, can also affect someone's competence' ([Health and Safety Executive, n.d.](#)). Moving into the forensic science domain, The European Network of Forensic Science Institutes (2011 p.3) define competence as 'the ability to perform the task of a certain role. A competent person has the knowledge and the ability to apply this knowledge, has the skills, the right behaviour and the attitudes for the role. Qualification, experience and training, although important, do not guarantee competence'. ILAC (2022 p.6) states 'competence is the demonstrated ability to apply knowledge and skills and, where relevant, demonstrated personal attributes'. [Rose \(2021\)](#) notes that it is also important that an individual is also able to demonstrate any requisite skills and knowledge consistently, and when being assessed against measurable criteria.

2.1. On a 'role' basis

In all parts of the investigative process, competency is essential for ensuring the overall integrity, reliability, and admissibility of any evidential findings produced for use in legal proceedings. Any DF organisation must ensure their staff are competent to perform the role and tasks they are required to do ([ILAC, 2022](#)). Competence is typically considered and evaluated on a 'role' basis - i.e. person 'x' may be considered a competent 'technician', and this is the case under accreditation frameworks such as ISO/IEC 17025:2017 (discussed further in Section 3.1). Emphasis is placed upon a need for clarity in terms of the scope of any role so that it is clear what competencies are required of those seeking to be competent at it ([ILAC, 2022](#)). In achieving competence for a given role an individual will maintain a series of necessary competencies ('the knowledge, skills, abilities, and behaviours') ([Vitello et al., 2021](#)) that allow them to perform at an acceptable level ([National Institutes of Health, n.d.](#)).

The [College of Policing \(2024b\)](#) notes that all DF practitioners must be 'competent in analysing a problem, breaking it down into component parts, interpreting large quantities of numerical data and determining and implementing the appropriate action' ([College of Policing, 2024b](#)). Further, in fulfilling their roles, it must be stressed that while DF professionals must have technical competencies ([Irons and Konstadopoulou, 2007](#)), competence must go beyond merely understanding technology and relevant cognitive competencies are of equal importance ([Neuteboom et al., 2024](#)).

Competency in DF encompasses a range of skills, including technical acumen, analytical proficiency, and an understanding of legal standards and ethical considerations. Competency within a role could also be demonstrated with more abstract technical knowledge such as having an understanding of the uncertainty of measurement (UoM) of DF tools. Although digital evidence is often perceived as objective and credible, there is a range of possible errors and uncertainties inherent in the evidence itself ([Casey, 2002](#); [Overill and Silomon, 2012](#); [Kiltz, 2020](#)), and software and hardware vary in capability and importantly their limitations. Understanding UoM in DF is achieved through everyday practice

and detailed tool verification/validation activities conducted as part of method validation testing. A recognition of sources of uncertainty, can identify potential errors in data collection or analysis processes (Casey, 2002; Overill and Silomon, 2012; Kiltz, 2020). This allows corrective measures or alternative techniques to be used, improving the overall reliability of results and through understanding measurement uncertainties in digital forensics, this enhances the accuracy, credibility, reliability, and integrity of forensic investigations, which is essential for providing robust and defensible digital evidence in various legal and investigative contexts.

2.2. 'Forensics' not 'investigation' - a focus on ISO

Focusing briefly on England and Wales, DF organisations evidencing competence within their laboratories must align with the requirements set out within ISO/IEC 17025:2017. When operating within ISO/IEC 17025:2017, the need to demonstrate competency focuses upon the 'forensic' parts of the work being conducted. To explain, forensic activities for the purpose of ISO accreditation can be divided into two distinct areas - the 'Capture and Preservation' and 'Processing and Analysis' of data (UKAS, 2024b). Capture and preservation is a crucial part of the DF process as legal and technical reasons may mean only one attempt is given to acquire any target data. Following the Forensic Science Regulator Code of Practice Section 82.3b - analysis can be described as 'the process of targeting digital data via a predefined and prescriptive forensic strategy' and involves actions and methods performed on data that help describe facts, detect patterns, develop explanations and test hypotheses. This includes keyword searching, the application of date filters and timelining, identification of files by known hash comparison, identification of data by algorithm e.g. nudity, image recognition, and the manual selection of data or files which is presented to the customer.

Within these activities, documented procedures are used by personnel to follow agreed and validated steps, and this may be a subset of what is required overall for a digital investigation. When these written procedures cease and professional judgement and investigative skills take over, this is where an 'investigation' begins, and this is not formally part of the accreditation approach. The 'investigation' element often involves the interpretation of data and sometimes can lead to opinion being presented to court. Whilst this can be UKAS assessed and accredited to ISO/IEC 17025:2017, at the time of writing no UK based DF laboratory is accredited (see UKAS's accreditation search for <https://www.ukas.com/find-an-organisation/>). It is described in the Forensic Science Regulators Code as a sub-activity with interpretation of any data or output with the purpose of providing opinion to include, but not be limited to, the following.

- i. Provenance or integrity of files/data. User activity (e.g. file creation, patterns of use);
- ii. Reliability/accuracy of data (e.g. recovered timestamps/GPS locations);
- iii. Effect of any virus or malware presence; and/or
- iv. Whether steps had been taken to conceal data (e.g. file manipulation).

Additional compliance to UKAS publication document LAB-13 is also required, which adds a layer of complexity to this skill. Therefore mainstream UK industry practice has been to deal only with the facts of the case and present results without opinion. The forensic element of any DF work encompasses only the following and application of technical procedures where an important part of competency evaluation in an ISO accredited environment is the ability to follow the approved documented procedures.

It is important to stress that whilst in England and Wales, accreditation may not require competence to be demonstrated for 'investigation' tasks, practitioners should still be competent to undertake these activities and organisations should take steps to ensure their staff can do this

work effectively.

Despite the requirement for ISO/IEC 17025:2017 having attracted criticism (Jones and Vidalis, 2019), it has arguably formalised the process of needing to address and document individual competence. Prior to its deployment, the recording of competence may have been approached in a more ad-hoc and informal manner, and possibly not have been given the attention that it required; competence has now been brought to the forefront of a DF organisation's attention. What is important to state is that the imposition of a need to adhere to accreditation frameworks has not brought with it the need for competence, practitioners have always needed to be competent, it has merely clearly defined the principles surrounding how it is to be achieved and demonstrated. In contrast, in jurisdictions and environments where ISO accreditation is not required or adherence to alternative standards is needed, methods for achieving it and the obligations for evidencing and evaluating competence may differ. Reference is drawn to Interpol's (2019) 'Global guidelines for digital forensics laboratories' as an international example of laboratory guidance including coverage of competence.

2.3. 'Competent' individuals and 'proficient' laboratories?

In the field of DF, we can arguably define two main components for quality management; the laboratory, and its staff (the 'practitioner'). At a practitioner level, we are often seeking to determine and assess their competency - 'a set of observable and measurable behaviours that are indicative of practical performance in a particular role' (Deloitte, 2017 p.20). As previously stated, competency is often considered in reference to a specific role (AG5, 2023; Europol, 2024), but it is argued that it may also be applied to a specific task or activity if a role is particularly broad, or a task/activity if it is particularly complex. Organisations may define a competency framework which outlines the skills, behaviours and knowledge required of individuals to fulfil specific roles (Deloitte, 2017). Competency may be thought of as 'an essential foundation for proficiency' (Veritas Asia Pacific Pty Ltd, 2022; AG5, 2023), and whilst being competent means an individual possesses the necessary attributes for a role, being proficiency implies an individual has mastery of them (Government of Canada, 2021; NIST, 2023). In a hypothetical operational environment, an individual may be considered a competent DF examiner and proficient in the use of a specific tool or technique. In all cases, those working in DF must be competent, and strive for proficiency within their roles.

When considering DF laboratories, within an ISO accredited environment reference is made to the term proficiency which refers to the overall capability of the laboratory to produce accurate, reliable, and consistent results. It encompasses the quality and accuracy of the laboratory's outputs in its entirety. There is a requirement for ISO/IEC 17025:2017 accredited laboratories to participate in proficiency testing. A subsequent ISO Standard is available for the establishment of competency for providers of such tests, namely ISO/IEC 17043. In line with this, an organisation must understand what their service level agreements (SLAs) define, allowing them to be clear on what they are offering, and in turn what any client/customer is expecting as a service.

3. Elements of competence

When attempting to establish the presence of competence for a hypothetical role, it is suggested that there are three core components that exist.

1. *Scope of competence*: The role that someone is seeking to (or claiming to) be competent at must be clearly defined.
2. *Competence threshold*: The level of skill that someone must achieve in order to be considered competent for a given role must be established and accepted.
3. *Evidence of competence*: The information that someone is relying upon to demonstrate that they are competent to conduct the role they are

claiming to be competent at. This may include the results of having completed a competence assessment, defined by The European Network of Forensic Science Institutes (2011 p.3) as ‘a formal assessment to check whether or not an individual meets the standards of performance’.

Each of these components is discussed in turn below.

3.1. Scope of competence

Perhaps a logical place to commence when considering the scope of competence is to determine the role that is being undertaken. In DF there are several roles, each requiring an individual to have specific competencies in order to fulfil them properly, but it is up to a DF organisation to define the roles that fit their organisational requirements, and the scope of them (ILAC, 2022). Governing organisations or professional bodies may provide guidance that helps to define DF roles in general, but different entities may define roles differently (see the College of Policing’s (2024c) role definitions as an example), or define roles that do not fully fit the requirements of an organisation. There is no overarching accepted and adopted set of role specifications in the DF field, however generally, roles may include the following.

- **Technician:** The ‘technician’ role traditionally should have skills that include case administration, exhibit/item handling and pre-imaging, photography, and capture and preservation of data (data acquisition/imaging). In some cases, they may also conduct ‘initial processing of digital evidence and be involved in triage and early decision-making’ in regard to seized devices (College of Policing, 2024c). A formal definition of the technician role has been provided by the College of Policing (2024c) and this can be accessed via their Professional Development Platform.
- **Examiner:** An ‘examiner’ role works with the acquired forensic Image (RAW or E01 files), completes technical processes and conducts analysis of data using forensic software. Typically, examiners ‘will report factual evidence based on the validated scientific methodology’ (Forensic Science Regulator Code of Practice section 28.2.1).
- **Investigator:** The ‘investigator’ conducts the digital investigation and provides the evidential report or statement. Whereas the ‘technician’ and ‘examiner’ roles fall within the ‘forensic’ category of work (see discussion in section 2.2), the ‘investigator’ role falls within ‘investigation’ within the eyes of ISO lab accreditation. Investigators ‘provide evidence, including opinion based on their practical experience and/or their professional knowledge’ (Forensic Science Regulator Code of Practice section 28.2.4).

Whilst there may be some overlap between roles or core functions (for example, those in every role should have competence regarding exhibit handling and continuity processes), and often elements of backwards compatibility will be present, due in part to individuals ‘moving up through the ranks’ as their career progresses, each role should have its own competency requirements. The roles may also be interchangeable in DF teams.

3.2. Role-scope

Clause 6.2.1 of the ISO/IEC 17025:2017 states that ‘all personnel of the laboratory, either internal or external, that could influence the laboratory activities shall act impartially, be competent, and work in accordance with the laboratory’s management system’. We have acknowledged competency is considered at a role level, however in disciplines such as DF, a concern could be raised as to whether considering competence in this way may pose in some cases a quality risk. Competence is not an all encompassing concept, and as a most dramatic example, it is difficult to envisage that a single entity can be considered competent at ‘digital forensics’ - this domain is simply too vast to

realistically claim competence in its entirety (Horsman and Shavers, 2022).

Given the complexity of forensic science and the specialisms that exist within them, some tasks may only have a few individuals that may be considered competent to undertake them (Kinder and Pirée, 2020). As a result, organisations must arguably be more fine grained when trying to define the boundaries of an individual’s scope of competence and role. If we consider the use of role-based competence, this time in reference to the generic roles noted above, can for example, an individual be such a thing as a competent technician?

Arguably, the answer is ‘yes’ providing that it is clear what is expected of a technician and the tasks and activities are defined clearly, from which the scope of a technician role could be expanded gradually when required. To explain further, given the vast array of devices and scenarios that could be faced, no technician can possess the requisite competence for all the potential technical circumstances that they could face. This position could be somewhat problematic in an operational reality if an organisation decided to address this position by creating hundreds of ‘micro roles’ with each dealing with isolated pockets of required competence for bespoke tasks. For example, this could see the presence of roles which are driven by specific techniques or devices, leading to roles such as an ‘iPhone technician’ or ‘MacOS technician’. However, the reality of the situation is that typically expansion elements of roles (for example, a technician may become competent at MacOS acquisitions) become ‘bolted on’ and are signed off by the relevant laboratory authority and updated on their quality management system.

In addition to defining roles with the necessary detail, processes should also be in place that describe what should be done when an individual is faced with a task that is beyond their remit. Being competent entails an individual being able to recognise such situations and follow the necessary procedures to flag such an event. Whilst the use of the term forensics may invoke feelings that practitioners require wide-ranging competency, this may in fact not be the case. Within the remit of accredited standards such as ISO/IEC 17025:2017, especially with the ‘forensic’ element of a digital investigation, simply following a procedure is now considered ‘competent’. This brings us to consider competency at a ‘task’ level.

3.2.1. Task-based competence

Within any single DF role, an individual will be expected to conduct one or more of the following activities.

1. **A single action:** Simply put, this may involve any single entity task as part of any of the stages of the DF investigative process. At the most simplest level of competence, for example a practitioner may demonstrate their ability to connect a mobile device to a forensic tool - a single action (in reality, a single task that is unlikely standalone).
2. **A method:** The Forensic Science Regulator (2020) defined a method as ‘a logical sequence of procedures or operations intended to accomplish a defined task’. Within any DF organisation, multiple documented and validated methods may exist for use across the spectrum of stages of a DF examination. Following the example above in (1) a practitioner may proceed to obtain competency to acquire the contents of the mobile device using a specific tool and extraction process.
3. **A process:** Within the confines of this work, we consider a process to contain multiple methods/actions which are combined to accomplish an investigative requirement. Finalising our example, a practitioner may examine the extracted contents of a mobile device and report upon any findings. This process absorbs a number of single actions and methodological competencies.

When a practitioner is claiming competence for a role, they are effectively claiming to be competent for subsets of activity that exist within the role’s scope. Defining a scope of competence is important to both the competence seeker or claimer, and to any third party wishing to

engage them in an activity which they are claiming competence for. For a competence seeker/claimer, it is important to understand those activities which they are seeking to or actually able to perform to an acceptable level. Simply put, professionals must know their limits ([The European Network of Forensic Science Institutes, 2011](#)), and operate within them if their practice is to be deemed safe and acceptable. In DF, defining the boundaries of any sought/claimed competence helps to ensure that a practitioner operates within their competency and not outside of it ([The European Network of Forensic Science Institutes, 2011](#)). It also helps prevent competency from being misstated or misrepresented ([Australian and New Zealand Forensic Science Society, 2021](#)). In addition, a defined scope of competence allows any third party who may seek to commission a DF practitioner to understand what they are capable of and therefore whether they can rely upon them to undertake the work that they require ([Australian and New Zealand Forensic Science Society, 2021](#)).

3.2.2. Specific competencies - method validation

Laboratories and their staff may require competency in some very specific areas of DF, one being method validation; the process used to confirm that any investigative procedure used for a specific examination is suitable for its intended use. Validation is the process of providing objective evidence that a method, process or device is fit for the specific purpose intended ([Forensic Science Regulator, 2020](#)). Competency in this activity requires comprehensive understanding of DF tools and their use, and knowledge of file and operating systems. A high level of accuracy is required with method validation studies and attention to detail to identify any discrepancies or errors. Method validation explores the accuracy of results generated by any methodology by considering both systematic and random errors ([Horsman, 2024](#)). Therefore critical thinking with the analysis of findings and comparison of forensic tools and side-by-side observations for proof of accuracy (trueness and precision) are important skills. Establishing the uncertainty factors that affect forensic tool performance and being able to express those factors in legal proceedings or reports another specific competency. Understanding the uncertainty of a tool can be through the robustness of the exercise and use of ground truth data with simulated case data to establish limitations.

Infrequently used techniques may pose a challenge in maintaining competence and capability for service providers and the use of such requires appropriate safeguards (FSR Code, 30.14.1). Being able to work without documented technical procedures or standard operating procedures with a thorough comprehension of the field that incorporates both theoretical and practical knowledge. For DF, this means a high level of competence in forensic principles and methodologies with an ability to adjust to novel and unforeseen circumstances, all the while upholding a high calibre of work.

3.3. Competence threshold

For someone to be competent for a given role, it is necessary to identify what 'competent performance' looks like ([The European Network of Forensic Science Institutes, 2011](#)). Whilst artificial, it is perhaps easiest to consider this as a linear scale in order to demonstrate this point ([Fig. 1](#)). Being competent for a specific activity does not necessarily

mean that an individual is capable of performing it perfectly, more that a performance is considered acceptable for that given task.

Only when acceptable performance for a task is known, can anyone be considered competent doing it, and the task of determining it can be time and resource intensive, and involve trial and error testing.

3.4. Evidence of competence

ISO/IEC 17025:2017 requires DF organisations to maintain demonstrative evidence of staff competency and their approaches to competency assessment and evaluation. Such processes must be recorded in an appropriate quality management system with easy access. To be competent, is to prove competence and concerns in DF over an inability of laboratories to evidence competence has been raised.

'A common finding raised was that DFUs did not have objective evidence to demonstrate the competency of their staff, other than relying on staff attending courses and having x years of Experience. Another common finding related to DFUs not having a mechanism to demonstrate on-going competence once individuals had been initially deemed Competent' (Tully et al., 2020 p.5).

Ballantyne and Wilson-Wilde (2020, p.3) state that 'in demonstrating competence, as in demonstrating validity, only empirical evidence can suffice. Although extensive training, years of experience or level of study are commonly used as proxies for competence, a true demonstration that a practitioner can produce accurate opinions can only be through blind testing on ground-truth known items. A practitioner should be able to provide evidence that they have been tested under conditions similar to those encountered in casework, and using the systems, processes and procedures in place, have obtained correct answers'.

If a claim for competence regarding a role is made, it must be supported by objective information that supports such a claim, the absence of which provides an unsatisfactory position. Forensic laboratories must maintain suitably detailed records that evidence the competence of their staff and the elements that make up this competence ([Forensic Science Regulator, 2023](#)). The absence of evidence to provide competence does not make an individual or entity incompetent per se, but it will impact the trust and reliance that should be placed upon it. Arguably in forensic disciplines, recipients of any forensic services must be able to trust the work they receive, placing an onus on the provider of such services to show they are capable of conducting such work effectively. Therefore whilst in theory, an individual who cannot prove their competence may in fact be competent, in the eyes of those involved with forensic science and those seeking their service, they may be considered incompetent.

Under ISO/IEC 17025:2017 competency must be evidenced following the completion of training. This can be through supervisory monitoring in test cases, review of technical records, professional discussion and question & answer sessions. Usually based upon documented and defined core skills for their role or activities. An evaluation and approval of someone's competency is usually fully documented and recorded in a quality management system as evidence, which is available for independent review usually by UKAS, but this can be requested for review by their customers.

Digital forensic laboratories around the world typically employ a combination of methods to ensure and prove the competency of their staff. Often, the certification of an individual by independent professional bodies is common practice. Some widely accepted certifications in the field of digital forensics include.

- Certified Forensic Computer Examiner (CFCE) from the International Association of Computer Investigative Specialists (IACIS).
- Certified Computer Examiner (CCE) by the International Society of Forensic Computer Examiners (ISFCE).
- GIAC Certified Forensic Examiner (GCFE) from the Global Information Assurance Certification (GIAC).
- EnCase Certified Examiner (EnCE) offered by OpenText.

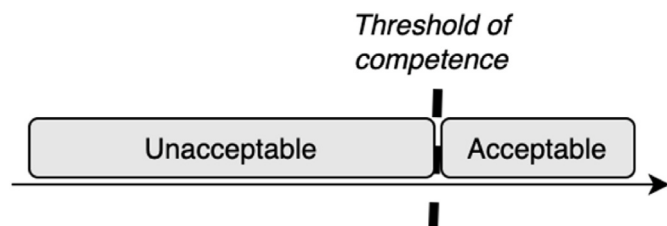


Fig. 1. Competence threshold.

- ACE - from Exterro are certified credentials that demonstrate the user's proficiency with Exterro's Forensic Toolkit (FTK).

3.4.1. 'The person'

Section 28.1.2 of the Forensic Science Regulator (2023) Code of Practice states that 'forensic units shall determine the appropriate local or nationally devised competence framework for practitioners which includes education, qualification, training, including statement/report writing and courtroom skills, technical knowledge, skills and experience, the nature of the competence assessment; the frequency of reassessment of competence; and whether observation of any testing or examinations are required, and if so, the frequency of this'. It is left to the responsibility of the forensic unit/laboratory to ensure that their personnel have the competence to perform laboratory activities (procedures) and to evaluate the significance of deviations. Following a set procedure is good practice in forensics, because this provides a consistent and repeatable scientific approach to examinations, plus most likely tried and tested as well as validated; however, where an item under examination poses a problematic technical difficulty (which is often the case in Digital Forensics) a set procedure may not be sufficient and deviating from normal practice the only option. This may be an infrequent or entirely novel procedure. A practitioner's understanding of the legal challenges and ramifications for such a deviation and potentially non-conforming work requires evaluation. Not following the steps outlined in the, such as improper evidence handling, incorrect application of forensic tools, or failure to maintain the chain of custody may render evidence unacceptable.

Organisations should consider deploying techniques (and documenting the use of these) that allow for a portfolio of competency-evidencing information to be acquired regarding the performance of an individual. This may include the following.

- *Shadowing*: Shadowing involves an individual observing the conduct of a competent colleague (Dolliver et al., 2017). Any organisation utilising shadowing as part of demonstrating competence of an individual must pay attention to the following-
 - the amount of shadowing;
 - the tasks being shadowed, and;
 - the frequency of shadowing.
- *Self assessment/reflection*: Practitioners should maintain records of their own experiences, any impact it has had upon their practice and any remedial actions which may have been put in place as a result.
- *Peer review*: The importance of peer review in DF cannot be understated (Horsman and Sunde, 2020; Sunde and Horsman, 2021). Peer review involves an assessment of any given work to determine its quality and reliability (The European Network of Forensic Science Institutes, 2011). Individuals can also be reviewed in terms of their behaviours and progression.
- *Case review*: The work practitioner may be subject to review. Arguably this goes beyond peer review, and includes a secondary and potentially blind investigation to allow an assessment of the practitioner work to be undertaken.
- *Mistakes made and corrections*: A formal record of any mistakes made by a practitioner and the ways in which these have been corrected should be maintained.
- *Independent assessment bodies*: CiiSEC (Chartered Institute of Information Security) and ICDIP (Institute of Cyber Digital Investigation Professionals) are examples of professional bodies that provide independent evaluation and assessment of the individual. Membership promotes and represents professionalism. An emphasis is in core skills where integrity and excellence of those operating within cyber digital investigations is demonstrated in a scrutinised (independently and impartially) in a portfolio of work. ICDIP exists to professionalise UK Law Enforcement and others who undertake or support cyber digital investigations.

Organisations must also assess the competence of their practitioners in their procedures. A competency assessment is 'a formal assessment to check whether or not an individual meets the standards of performance' (The European Network of Forensic Science Institutes, 2011). ISO/IEC 17025 requires laboratories to periodically evaluate and ensure the competency of their personnel in performing specific tasks, using specified methods, and understanding quality system policies and procedures. A discussion of the timing of assessments is reserved for Section 3.4.3 The testing of competency must be a fundamental component of an individual's forensic training 'and is administered as part of a comprehensive assessment of technical skills and knowledge during basic training, and prior to the initiation of case work by a forensic science practitioner on a newly validated technology, technique, or method' (National Commission on Forensic Science, 2016 p.6). Being able to keep a watch on newly updated forensic software for errors and bugs then troubleshooting is a primary skill-set in DF. The types of competency test an organisation may deploy include the following.

- *In-house & independent evaluation of competency*: Conducting assessments in-house can be more cost effective and significantly reduce expenditure compared to outsourcing to third-parties. Conducting evaluations in-house can aid in identifying skill gaps and providing training opportunities for improvement, as well as identify concerns about compliance with industry standards and best practices. In-house evaluations allow for tailoring assessments to specific organisational needs and requirements. Organisations have more control over the evaluation process, ensuring it aligns with their standards and objectives. In addition immediate feedback can be given which provides swift identification of areas for improvement or confirmation of strengths and compliance. A strong argument with private forensic service providers may be that internal assessments may help in maintaining the confidentiality of sensitive information and data.

However, conducting In-house evaluation can be problematic as internal evaluators may exhibit bias or lack objectivity, potentially skewing the assessment results - 'friends assessing friend making for subjective assessments'. Potential conflict of interest may arise when evaluating peers, colleagues or subordinates. Leading to a compromise with the integrity of the evaluation process. Managing evaluations internally can be time-consuming and resource intensive, leading to arguments that it distracts from core operational activities. A lack the necessary expertise to conduct comprehensive evaluations in-house makes the assessment process flawed and technical details overlooked.

Using external independent evaluators brings additional experience, but also alternative viewpoints, and diverse perspectives that may be lacking in in-house assessments. However, sensitive company or business information may be exposed to an external evaluator requiring comprehensive assurances, non-disclosure agreements and compliance with legal and regulatory measures.

- *Simulated casework*: An organisation may produce or stimulate case work and evaluate a practitioner's performance when engaging with it.
- *Direct observations*: Suitably competent staff may directly observe the conduct of an individual when performing their role and record their findings (ILAC, 2022).

Whilst it may seem obvious to state, those who assess competence must be competent/know what competence is for that given task (The European Network of Forensic Science Institutes, 2011; Rose, 2021).

3.4.2. A word on training

DF organisations often utilise training courses in order to support the development of their staff, however, it is important to stress that an individual's attendance on many training courses does not make them automatically competent. Training can be considered a building block, a

crucial part of an individual building competency, but engagement with training alone is not evidence of competency. Training focuses on the learning process, while competency focuses on the application and demonstration of learned skills and knowledge. Training focuses on the delivery of information and teaching skills, whereas competency is about evaluating the ability to perform tasks correctly and reliably. Training may have a defined duration such as a workshop or a course, whereas competency is an ongoing requirement and one that requires periodic reassessment. The outcome of training is to have the necessary knowledge and initial skills. The outcome of competency is the verified ability to carry out tasks properly under actual working conditions. Under ISO/IEC 17025:2017, laboratories must ensure both training and competency of their personnel; the standard requires that laboratories have processes in place for identifying training needs and providing training. DF organisations cannot rely on training alone to demonstrate competency as doing so would be to assume that everyone is a competent learner.

3.4.3. Time

The field of DF is in a constant state of flux and development, and as a result competency must be maintained as equipment, techniques and investigative methods develop and change (Rose, 2021). In England and Wales, this is acknowledged by the Forensic Science Regulator Codes of Practice who states that all persons undertaking forensic work are required to be 'deemed competent, and this competence is maintained and monitored' (Forensic Capability Network, n.d.). Competence is not a static thing (General Chiropractic Council, 2024), where those who achieve it must continually work to maintain it, and, be reassessed at appropriate periods to determine if they can still perform at an acceptable level (see Fig. 2). An individual's competence may wax and wane as a result of external impactful factors, for example, a temporary secondment or role change may cause a loss of competence, which may need to be addressed via a period of training/re-learning. In turn, time in general may impact performance as bad habits may creep into practices, along with biases and general error.

The impact of time upon competence may vary depending on the role being undertaken and what a person is doing. However, the FSR Code of Practice (2023) notes at section 28.1.3a DF organisation must have processes in place that address situations when a practitioner's competence is found to have either lapsed, not been demonstrated or in the event that their credibility is undermined. It should be stressed that the period of time between when competence is established and any re-evaluation of it must be considered dynamic and frequency of re-evaluation based upon risk. Any decisions to re-assess the competence of a person should be driven by the management of risk posed by failing to do so to the proficiency of the service offered by the forensic laboratory. Laboratory quality management systems have a balance to strike when re-assessing competence; too often and they risk paralysing the

performance of those within the organisation and therefore the productivity of the business itself. Too infrequent, and persons may be conducting duties incompetently, unbeknown (see Figure). The goal of tracking competence is to attempt to identify or intervene at a point where competence may be at risk of being lost, whereas a minimum, competency re-evaluation argued as yearly and many laboratories do conduct this annually. This is a common practice to ensure that staff maintain the necessary skills and knowledge; however, there is no universally mandated minimum frequency for competency re-evaluation in digital forensic laboratories, best practices and guidelines generally suggest this. Under ISO accreditation (17025/17,020) this is not defined and the laboratory could theoretically take a more risk based approach to establishing competency with their personnel. This could be extended to once over their four year accreditation cycle (re-assessment is conducted then), and evidence of competency again comes under scrutiny. Alternative evidence sources such as existing peer or quality reviews of casework, audits and participation in Proficiency Testing (or inter-laboratory tests) could be supplemented as evidence of competency. Risks do become more unmanageable the longer the periods of re-evaluation and organisations need to carefully record this, and be in a position to justify or mitigate as accreditation suspension could be the result of competency failures.

As a hypothetical example, a small close knit team performing the same business as usual tasks daily will require less frequent re-evaluation, especially if they have other supporting controls in place, such as peer review checks, quality checks, participation in proficiency testing, involvement in method validation and tool verifications/validations. Whereas a larger team populated with more junior newer staff poses a higher risk and more frequent competency evaluations may be considered better practice.

3.4.4. Proficiency testing - 'the lab'

In 2020, Tully et al. raised serious concerns in relation to competence in labs. Proficiency testing 'allows the introduction of samples of known but undisclosed content into a laboratory's routine testing procedure' (Gov.uk, 2015) which help to assess its performance. In the context of forensic science, proficiency testing is not intended to assess individual competence (National Commission on Forensic Science, 2016), instead 'participant performance against pre-established criteria' (ISO/IEC 17043:2010).

UKAS's (the national accreditation body for the United Kingdom and assessor of ISO/IEC 17025:2017 in DF laboratories in England and Wales (UKAS, 2024a)) document TPS-47 (UKAS Policy on Participation in Proficiency Testing) states 'ISO/IEC 17025:2017 requires laboratories to have procedures for monitoring the validity of results. It is also clear that laboratories shall monitor their performance by comparison with results of different laboratories where available and appropriate. This will include either or both of proficiency testing or other interlaboratory comparisons. These methods provide a mechanism for a laboratory to demonstrate its competence to both its customers and the accreditation body'. Proficiency testing in respect of ISO/IEC 17025:2017 is that this is a test of the laboratory and not the individual.

Proficiency testing can be considered and conducted in the following three ways.

1. **Independent proficiency testing (IPT):** IPT may be considered the 'gold standard' in terms of testing. An independent organisation or party may produce data or an investigative scenario where acceptable performance for examining it is known. An organisation seeking to assess competence within their organisation may purchase a test(s) and deploy it within their environment, and once complete, return it for independent evaluation. Any IPT provider must themselves be competent to provide a proficiency testing service, where in England and Wales, those organisations may evidence their own competence to provide a testing service by seeking accreditation against ISO/IEC 17043:2023 - 'conformity assessment'. These services will incur a

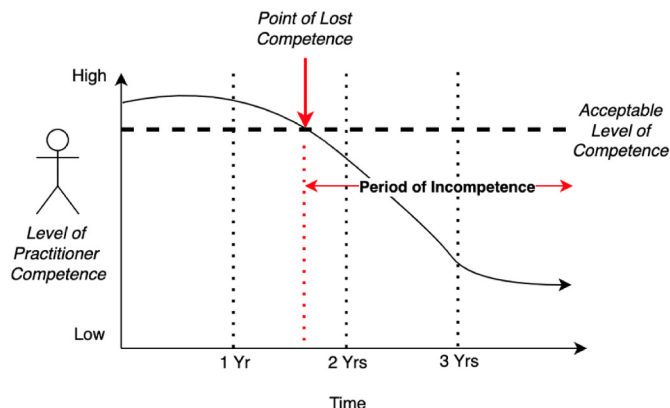


Fig. 2. The impact of time on competence - natural degradation.

cost, but arguably, the expense of these services should not be considered sole justification for not utilising them.

2. *Interlaboratory comparisons (ILCs)*: ILCs involve an agreed relationship between two or more laboratories to create and share 'tests' which the other party can attempt to solve within the bounds of their current accepted laboratory procedures. In comparison to IPTs, this may not be a paid for service and one that may hinge upon goodwill and a general acknowledgement of a 'need' for it. ILCs have value in the remit of competency testing, but they are time consuming, resource intensive, and just with IPTs, require a level of competence in order for them to be created properly.
3. *Blind tests*: Where all else has been reviewed and either not available or suitable as a test, a laboratory may as a last resort opt for other inter/intra-laboratory comparisons e.g., analysis of blind samples within the laboratory. Strong justification needs to be documented and all other types ruled out.

In relation to ISO/IEC 17025:2017 accreditation, TPS-47 section 4.2 states that 'laboratories and inspection bodies are required to investigate scheme availability and also determine the appropriateness of the scheme'. Any produced tests should try to be realistic and represent the problems that will be faced by a DF laboratory and test end-to-end processes with an aim of establishing whether they are both correct, and performing correctly and the tests themselves may delve as deep and far into a DF labs functionality as they like. The outcome of proficiency testing is either pass or fail. With UKAS accredited laboratories, any significant unexpected results from tests may require escalation as a report to the Forensic Science Regulator, or at least raise internal non-conformity reports where a root cause and extent investigation is necessary. Improvement actions from this are to prevent recurrences and improve quality.

4. Risks of incompetence

Discussions concerning competence may cause feelings of unease, particularly when reference to incompetence is raised. It is necessary to stress that just because someone may not be competent in a certain task or procedure, this does not necessarily make them totally incompetent. However, it is necessary to emphasise that those who lack competence for a role are essentially considered incompetent. The presence of incompetence within DF lab environments poses a number of risks at various levels of severity ranging from simple administration errors to missing vital information during examination processes and the loss of evidence. Reputational damage remains one of the most severe risks for organisations operating within this domain. The mishandling of or improperly collecting digital evidence can alter or destroy critical data, making it unusable in court. Failing to properly document the chain of custody can lead to questions about the integrity of the evidence, potentially resulting in it being inadmissible in legal proceedings. From something as seemingly innocuous as the mislabelling of an evidential item may risk inadmissibility in a court hearing, leading to serious questions regarding its legitimacy, integrity, and the examination rendered upon it. It may open up larger concerns that the incompetence demonstrated in a present example may be being replicated in other previous casework, casting doubt on previous criminal convictions or resulting in exoneration.

A significant risk with accredited laboratories is the raising of findings of ISO non-conformity on an assessment - areas where the laboratory is not performing as it should be when operating under a framework of accreditation. This could lead to suspension of laboratory accreditation by the regulatory assessment body (UKAS in the United Kingdom). Suspension is a reputational risk as this is publicly reported by UKAS on the sanctions section of their website. Furthermore, a declaration of unaccredited activities is required with all reports or statements which could cast doubt on the validity of evidence presented at court. Failure in this and continuance of providing an undeclared and unaccredited

forensic service could lead to offences against the Forensic Science Regulators Act 2021.

Incompetence can also increase the risk of security breaches. Mishandling sensitive data or not following proper information/cyber security measures could expose evidence via unauthorised access to systems or during a cyber-attack. DF is a different field to cyber security and competency in cyber related issues and risk is not traditionally assessed. There may be a natural assumption that DF practitioners are also competent with cyber security; but this may not be the case. If little or no training is provided to personnel in DF laboratories/Units regarding cyber security related issues, then an expectation of competence in these areas is problematic. The advent of clause 32 in the Forensic Science Regulator Code has provided a framework for DF units to follow and reduce risks and vulnerabilities in systems and software, but awareness of it or adherence to it may be limited. To provide a hypothetical examination, an argument may be cited that anti virus software may impact the functionality of forensic software and therefore be removed or restricted on laboratory systems. Doing so may pose a significant cyber security risk.

5. Discussions and conclusions

This work has discussed the concept of competence, the elements it comprises and the application of it within the field of DF. There is a natural gravitation to ISO/IEC 17025:2017 and the requirements for competence that it sets out which laboratories must adhere to in order to seek accreditation, and therefore some reflection is required here. Perhaps the first question here to raise is that whilst this standard sets strong competency requirements, it does so by focusing on the need to evidence a competent ability to follow documented technical procedure or standard operating procedures. This raises the question - is this really a true test of DF competency? We have noted that this standard focuses on the parts of an investigation that it defines as '*forensic*', a portion of tasks largely driven by technical documentation and defined practices, with investigative elements falling largely outside of its remit. Within this in mind, competency may be viewed as a simple ability to follow processes that have been set out without any unaccounted for deviation. Whilst this is an important skill within the forensic remit, it is perhaps not what most people would view as being the requirements for competence. Conversely, evidencing and assessing the remaining 'investigative' parts of the forensic process poses a significant challenge given the subjectivity involved in any decision making and justifications. In essence, adherence to ISO/IEC 17025:2017 does not guarantee an organisation has '*good investigators*', but it does help to ensure that they get the fundamentals of a DF examination right.

5.1. Are all tasks considered equal?

DF tasks can take a variety of shapes and forms and it may be necessary to consider if all are assumed to require the same levels of competence, and treated as such. Some subject areas in DF, such as Kiosk triage which is used remotely with mobile phone examinations have been perceived to require less competence. This may be partly due to the ways in which vendors market these products which are designed to be intuitive and used by individuals with limited technical expertise, making it easier for first responders and field officers to perform preliminary investigations ([Scottish Police Authority, 2023](#)). Such processes are in place to meet the increasing demand for triage, intelligence gathering and to gain immediate access to information in a custody suite environment. Such processes may also reduce backlogs of work for forensic units. Kiosks are often operated by non-forensic unit personnel, such as custody suite staff or digital media investigators, with limited training and overall DF skills. This poses an increased risk and in such cases organisations have struggled to achieve accreditation.

Whilst we have focused upon laboratory based DF practices, there are on-scene activities that vary in terms of techniques and range of

forensic tools used. RAM capture, network assessment, router downloads and scene preservation and management are tasks that may be considered more of a fit with ISO/IEC 17020:2012, an international standard that contains requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities. Tasks involve evaluating conditions, making professional judgments, and various other inspection-related activities. Competency requirements include the ability to interpret standards and regulations specific to what is being inspected. ISO/IEC 17020:2012 stresses the competence of personnel, including supervisors, decision-makers who interpret results and extends to personnel who can handle inspection procedures, make observations, interpret standards, and conclude conformity.

5.2. Expertise vs competence

Herling (2000), emphasises that competence is different to expertise. Whilst we have previously acknowledged that competency is related to the skills, knowledge and behaviours needed to perform a task well, expertise relates to above-average and outstanding domain-specific knowledge, experience, and problem-solving skills (Herling (2000)). Expertise is not simply a matter of how many cases someone has completed, or the number of years they have been a DF Investigator, nor are educational achievements, post-nominals, and seniority. Instead, it is a multifaceted concept consisting of a portfolio of evidence that when taken together provides evidence that someone has mastery of a given task, process or role.

Expert witnesses must satisfy the threshold legal test of competency before being allowed to testify or submit an expert report in legal proceedings (see Criminal Practice Directions, 2023 Section 7). To ensure evidence is reliable and relevant, courts in England and Wales test and apply guidelines to establish that the competency and admissibility of evidence from forensic expert witnesses is acceptable. Primarily based on qualifications, experience, and ability to provide impartial and informed opinion evidence. An expert must have the necessary expertise in DF and can be shown through peer recognition, academic qualifications, and professional experience. Part 19 of the CrimPR (Criminal Procedure Rules) also deals with expert evidence, placing an emphasis on the duty of experts to help the court on matters within their expertise. Together with the requirement for comprehensive and clear reporting. Whilst individuals may be described as experts or class themselves as such, it is a matter for the courts to decide upon the expertise status of a DF practitioner in trials. Clear knowledge of the issues directly related to the case, explaining critical findings with a necessity to disclose any limitations in analysis, and the obligation to avoid and disclose conflicts of interest. Providing insights that the judge or jury would not likely possess without such testimony is the purpose of expert testimony, aiding the court while maintaining impartiality and integrity. These latter being two key factors in the procedure rules.

When the DF practitioner offers opinions and interpretations as evidence, a higher level of competency and experience is expected. Importance is placed in the assertion that the inferences are logically sound and that alternative hypotheses in the investigative opinion mode and alternative propositions in the evaluative opinion mode have been properly considered (Forensic Science Regulator, 2021). Experts may also need to explain their methodology and reasoning, and cite a body of current specialised literature relevant to their field of expertise, weighing its support or opposition to their methods. At the time of writing, all police DF units (in England & Wales) tactically avoid providing any opinions in their reports, and only facts are reported. It could be argued that in many cases, there is not a requirement to step outside of these bounds as any overarching matters may be considered straight forward. In turn, DFU practitioners may be rarely challenged in court and often suspects plead guilty when presented with the facts. When providing expert opinion, practitioners in the DF domain may look wider to more established areas of forensic science where

frameworks such as 'Case Assessment and Interpretation' exist to 'enhance examination strategies and inform evidential analysis and interpretation in relation to any kind of expert evidence received in criminal proceedings' (Aitken et al., 2010 p.13).

Competence is and will remain a crucial component of all DF work being undertaken worldwide. This work has emphasised the need for it and described the elements of it that any practitioner and the organisation must tackle when trying to document and evidence it. The current landscape regarding competency has been described with an emphasis placed upon describing what ISO/IEC 17025:2017 states and requires. Our intention is to add to the discussions surrounding competence and try to support by offering an insight into this topic and the requirements of it.

CRedit authorship contribution statement

Graeme Horsman: Writing – review & editing, Writing – original draft, Supervision, Project administration, Methodology, Investigation, Conceptualization. **Andrew Dodd:** Writing – review & editing, Writing – original draft, Methodology, Investigation, Conceptualization.

Data availability

No data was used for the research described in the article.

References

- AG5, 2023. Competency vs. proficiency: understanding the differences and their importance for skills development. Available at: <https://www.ag5.com/competency-vs-proficiency-understanding-the-differences-and-their-importance-for-skills-development/>.
- Association of Chief Police Officers, 2011. ACPO good practice guide for digital evidence. https://npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf.
- Aitken, C., Roberts, P., Jackson, G., 2010. Communicating and interpreting statistical evidence in the administration of criminal justice. Practitioner Guide (1).
- Australian and New Zealand Forensic Science Society, 2021. Code of professional practice. Available at: <https://anzfss.org.au/resources/code-of-professional-practice/#:~:text=Forensic%20practitioners%20who%20are%20members,employers%20and%203>.
- Ballantyne, K.N., Wilson-Wilde, L., 2020. Assessing the reliability and validity of forensic science – an industry perspective. Aust. J. Forensic Sci. 52 (3), 275–281. PAGE 3.
- Cambridge Dictionary, 2024. 'Competence' available at: https://dictionary.cambridge.org/dictionary/english/competence#google_vignette.
- Casey, E., 2002. Error, uncertainty and loss in digital evidence. International Journal of Digital Evidence 1 (2).
- College of Policing, 2024a. Digital intelligence and investigation – new learning modules. Available at: <https://www.college.police.uk/article/digital-intelligence-and-investigation-new-learning-modules#:~:text=More%20than%2090%25%20of%20reported,the%20UK%20practitioners%20of%20pounds>.
- College of Policing, 2024b. Digital forensic practitioner. Available at: <https://profdev.college.police.uk/professional-profile/digital-forensic-practitioner-draft/#:~:text=A%20relevant%20technical%20degree%20or,operating%20with%20an%20accredited%20environment>.
- College of Policing, 2024c. Digital forensic technician. Available at: <https://profdev.college.police.uk/professional-profile/digital-forensic-technician-draft/>.
- Collins, 2024. 'competence'. Available at: <https://www.collinsdictionary.com/dictionary/english/competence>.
- De Kinder, J., Pirée, H., 2020. The future of the forensic science providers–Time to rethink our structures? Forensic Sci. Int. 316, 110471.
- Deloitte, 2017. Competent or merely well informed? Available at: https://www2.deloitte.com/content/dam/Deloitte/xs/Documents/About-Deloitte/mepovdocument/mepovissue22/competent-or-informed_mepov22.pdf.
- Dictionary.com, 2024. 'Competence' available at: <https://www.dictionary.com/browse/competence>.
- Dolliver, D.S., Collins, C., Sams, B., 2017. Hybrid approaches to digital forensic investigations: a comparative analysis in an institutional context. Digit. Invest. 23, 124–137.
- Doyle, S., 2020. A review of the current quality standards framework supporting forensic science: risks and opportunities. Wiley Interdisciplinary Reviews: Forensic Sci. 2 (3), e1365.
- Europol, 2024. Cybercrime training competency framework. Available at: <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Cybercrime%20Training%20Competency%20Framework%202024.pdf>.
- Forensic Capability Network (n.d.) 'FORENSIC WORKFORCE STRATEGIC PLAN 2021/26' Available at: <https://fcn.lets-go.live/docs/forensic-workforce-strategic-plan-2021-2026finalpdf/download?attachment#:~:text=This%20plan%20sets%20out,a%20competence%20C%20and%20continued%20professional%20development>.

- Forensic Science Regulator, 2020. Forensic science regulator guidance method validation in digital forensics FSR-G-218 issue 2. Available at: https://assets.publishing.service.gov.uk/media/5f6ca608d3bf7f7231ac65e0/218_Method_Validation_in_Digital_Forensics_Issue_2_New_Base_Final.pdf.
- Forensic Science Regulator, 2021. Forensic science regulator Codes of practice and conduct development of evaluative opinions. Available at: https://assets.publishing.service.gov.uk/media/602407728fa8f5146f0769d9/FSR-C-118_Interpretation_Appendix_Issue_1_002_.pdf.
- Forensic Science Regulator, 2023. 'Code of practice'. Available at: https://assets.publishing.service.gov.uk/media/64da431cc8dee4000d7f1c1e/FINAL_2023.1.18_Code_of_Practice.pdf.
- Gov.uk, 2015. Proficiency testing: the process and benefits. Available at: <https://www.gov.uk/guidance/external-quality-assessment-eqa-and-proficiency-testing-pt-the-process-and-benefits>.
- Government of Canada, 2021. Competent vs proficient? Which are you? Available at: <https://tc.canada.ca/en/aviation/publications/aviation-safety-letter/issue-3-2021/competent-vs-proficient-which-are-you>.
- Health and Safety Executive (n.d.) 'What is competence?' Available at: <https://www.hse.gov.uk/competence/what-is-competence.htm>.
- Herling, Richard, 2000. Operational definitions of expertise and competence. *Adv. Develop. Hum. Resour.* 2, 8–21. <https://doi.org/10.1177/152342230000200103>.
- His Majesty's Inspectorate of Constabulary and Fire & Rescue Services, 2022. An inspection into how well the police and other agencies use digital forensics in their investigations. <https://hmicfrs.justiceinspectorates.gov.uk/publications/how-well-the-police-and-other-agencies-use-digital-forensics-in-their-investigations/#:~:text=We%20found%20that%20the%20demand,report%20sets%20out%20our%20findings>.
- Hoffmann, T., 1999. The meanings of competency. *J. Eur. Ind. Train.* 23 (6), 275–286.
- Horsman, G., Sunde, N., 2020. Part 1: the need for peer review in digital forensics. *Forensic Sci. Int.: Digit. Invest.* 35, 301062.
- Horsman, G., Shavers, B., 2022. Who is the digital forensic expert and what is their expertise? *Wiley Interdisciplinary Reviews: Forensic Sci.* 4 (5), e1453.
- Horsman, G., 2024. Sources of error in digital forensics. *Forensic Sci. Int.: Digit. Invest.* 48, 301693.
- ILAC, 2022. Modules in a forensic science process. Available at: <https://ilac.org/?ddownload=124605>.
- Interpol, 2019. Global guidelines for digital forensics laboratories. Available at: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics.
- Interpol, 2024. Digital forensics. Available at: <https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics>.
- Irons, A.D., Konstadopoulou, A., 2007. Professionalism in digital forensics. *Digital evidence & elec. Signature L. Rev.* 4, 45–50.
- Jones, A., Vidalis, S., 2019. Rethinking digital forensics. *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN 2516, 0281.
- Kiltz, S., 2020. Data-Centric Examination Approach (DCEA) for a Qualitative Determination of Error, Loss and Uncertainty in Digital and Digitised Forensics (Doctoral Dissertation).
- Le Deist, F.D., Winterton, J., 2005. What is competence? *Hum. Resour. Dev. Int.* 8 (1), 27–46.
- Losavio, M., Seigfried-Spellard, K.C., Sloan III, J.J., 2016. Why digital forensics is not a profession and how it can become one. *Crim. Justice Stud. Crit. J. Crime Law Soc.* 29 (2), 143–162.
- Muir, Rick, Walcott, Stephen, 2021. Unleashing the value of digital forensics. https://www.police-foundation.org.uk/wp-content/uploads/2010/10/value_of_digital_forensics.pdf.
- National Commission on Forensic Science, 2016. Proficiency testing in forensic science. Available at: <https://www.justice.gov/ncfs/file/831806/dl#:~:text=Competency%20testing%20is%20an%20integral,technology%2C%20technique%2C%20or%20method>.
- National Institutes of Health (n.d.) 'What are competencies?' Available at: <https://hr.nih.gov/about/faq/working-nih/competencies/what-are-competencies>.
- National Police Chiefs' Council, 2020a. National policing digital strategy. Available at: <https://pds.police.uk/wp-content/uploads/2020/01/National-Policing-Digital-Strategy-2020-2030.pdf>.
- National Police Chiefs' Council, 2020b. Digital forensic science strategy. Available at: <https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/national-digital-forensic-science-strategy.pdf>.
- Neuteboom, W., Ross, A., Bugeja, L., Willis, S., Roux, C., Lothridge, K., 2024. Quality management and competencies in forensic science. *Wiley Interdisciplinary Reviews: Forensic Sci.* 6 (3), e1513.
- NIST, 2023. Measuring cybersecurity workforce capabilities: defining a proficiency scale for the NICE framework. Available at: <https://www.nist.gov/system/files/documents/2023/10/05/NIST%20Measuring%20Cybersecurity%20Workforce%20Capabilities%207-25-22.pdf>.
- Overill, R.E., Silomon, J.A., 2012. Uncertainty bounds for digital forensic evidence and hypotheses. In: 2012 Seventh International Conference on Availability, Reliability and Security. IEEE, pp. 590–595.
- Rose, Andre, 2021. What is it to be competent? Available at: <https://www.imca-int.com/published-articles/what-is-it-to-be-competent/>.
- Scottish Police Authority, 2023. Cyber Kiosk update - 12 september 2023. Available at: <https://www.spa.police.uk/publication-library/cyber-kiosk-update-12-september-2023/>.
- Stockwell Safety (n.d.) 'The Importance of Competence' Available at: <https://stockwellsafety.com/health-and-safety-training-and-competence/>.
- Sunde, N., Horsman, G., 2021. Part 2: the phase-oriented advice and review structure (PARS) for digital forensic investigations. *Forensic Sci. Int.: Digit. Invest.* 36, 301074.
- The European Network of Forensic Science Institutes, 2011. Guidance on the assessment of competence for forensic practitioners. Available at: <https://enfsi.eu/wp-content/uploads/2017/11/QCC-CAP-006-001.pdf>.
- Trinder, J.C., 2008. Competency standards-a measure of the quality of a workforce. *Гео-Сибирь* 2 (S2), 9–14.
- Tully, G., Cohen, N., Compton, D., Davies, G., Isbell, R., Watson, T., 2020. Quality standards for digital forensics: learning from experience in England & Wales. *Forensic Sci. Int.: Digit. Invest.* 32, 200905.
- UKAS, 2024a. About us. Available at: <https://www.ukas.com/about-us/>.
- UKAS, 2024b. The UKAS summary forensic master schedule. Available at: <https://www.ukas.com/resources/technical-bulletins/the-ukas-summary-forensic-master-schedule/>.
- Veritas Asia Pacific Pty Ltd, 2022. What is more important, competence or proficiency? <https://linkedin.com/pulse/what-more-important-competence-proficiency-veritas-asia-pacific-pty-ltd/>.
- Vitello, S., Greateorex, J., Shaw, S., 2021. What Is Competence? A Shared Interpretation of Competence to Support Teaching, Learning and Assessment. Cambridge University Press & Assessment.



DSPACE

<https://dspace.org/>

Competence in digital forensics

Horsman, Graeme; Dodd, Andrew

2024-12-01

Elsevier

<https://doi.org/10.1016/j.fsidi.2024.301840>

Horsman G, Dodd A. (2024) Competence in digital forensics. Forensic Science International: Digital Investigation, Volume 51, December 2024, Article number 301840