DELIVERY PHASE

Output 4: Procurement and installation of equipment with full quality assurance oversight

On approval from the Authority, we will initiate equipment procurement. Overseen by the Torchlight Project Manager, Melissa, our Project Support Officer will coordinate all the logistics related to the purchasing and delivery activities, maintaining communication with the chosen suppliers and shippers to ensure that the equipment is delivered on time and in line with scope. Wherever possible we will conduct inspections of the consignments before they ship to ensure full alignment with the specified requirement. We have significant experience facilitating the shipment of equipment worldwide and maintain a network of international freight handlers who have extensive experience moving goods to challenging locations in fragile states. Our shipping agents understand the varying requirements for customs and maintain local representatives in each focus country to receive the consignment and oversee its clearance. We will work with the Authority to minimise the logistics chains supporting this project by sourcing supplies/equipment from local or regional suppliers wherever possible, both reducing import/export challenges as well as contributing to local economies.

Throughout the procurement, delivery and installation process we will maintain full quality assurance in line with our standard assurance policies and protocols, proven to be effective across numerous challenging equipment procurement projects. Key to quality is regular communication with all suppliers, enabling direct supervision and oversight over the entire process. Communication with the in-country leads will ensure that all necessary on-site preparations are in place prior to the shipment of the equipment. The delivery of the equipment will be coordinated to coincide with the delivery of the training at each location (see Output 3 below). Our input schedules allow for our Delivery Team to be on-site to conduct a full audit of the equipment and immediately identify any issues requiring resolution. The Delivery Team will conduct the installation and testing of equipment to ensure the equipment is fully functional. Our teams will advise end users on measures to maximise efficiencies of use through optimal configuration of the equipment. This will also help to improve efficiencies in overall workflow processes. During the installation period, there will be opportunities for our Delivery Team to train beneficiary IT managers/administrators on equipment installation and operationalisation, demonstrating how to set up the equipment, conduct routine maintenance and troubleshoot common issues. Guidance will also be provided on any manufacturer technical support that will be available to the end-users and how this can be accessed.

Updates will be provided regularly to the Authority Project Manager to ensure they maintain visibility and oversight throughout the stages of procurement, shipping and installation.

Output 5: Combining technical digital training with use in investigations to build a full spectrum operational capability

During the equipment procurement period, our expert teams will produce bespoke training materials based on the approved plan for each country. Each training programme will have three component parts: 1) digital evidence; 2) online investigations and 3) forensic awareness - digital evidence (Output 5). The first two components will be aimed at the digital evidence examiners and CT investigators—participation on the forensic awareness component will be extended to include prosecutors and judiciary, where appropriate (the examiners and investigators are expected to attend all three sessions). This 'combination training' provides technical upskilling in digital evidence examination and also supports wider awareness within the criminal justice system, fostering interoperability and a 'shared language' which experience has demonstrated accelerates uptake of new methodologies in support of improving justice outcomes.

For training delivery, we will use Blended Teams –each team will be led by the Digital Evidence Expert who oversaw the scoping and supported by expert CT Senior Investigating Officers (SIOs) Richard Southwell and Dave Bredo, both of whom are highly experienced at utilising digital evidence operationally as well as building capability. They will be further supported by a highly experienced CT Prosecutor, Asker Husain. Blending delivery of the specialist technical input (by the Digital Evidence Experts) with training in how digital evidence supports the wider CT investigation process (by the CT SIOs) and then deploying digital evidence during prosecutions (by the CT prosecutor). This approach will enable participants to a gain a full spectrum understanding of how digital evidence is used throughout a CT case – a critical understanding, which can be lost if the training is siloed or too narrowly focussed on the mechanical use of digital evidence tools. This pairing will also enable participants to better understand the role of the SIO in developing a forensic strategy for digital evidence and admissibility of digital evidence in court.

We anticipate delivering a block of 12 days of training per location, with an estimated 2 days of equipment installation (note that this may change depending on the selected equipment and agreed implementation plan). Given the operational context and the expected requirements for this type of training, all our course materials and practical scenario-based exercises will be based on localised and highly relevant Counter Terrorist (CT) threats, ensuring the training provides maximum and immediate operational uplift in a way tailored to the specific context of the CT threat in each location. Wherever possible, we will build in the use of existing tools/processes to the training. For example, the Maldives Police have been equipped with i2 Analyst Notebook and our trainers can incorporate this specific capability into the exercises to demonstrate how existing equipment/processes complement the new training/tools.

Human rights compliance is a golden thread throughout all our delivery. We use the AIMS process to assess human rights risks within our training and will identify specific safeguarding measures put in place to address human rights issues that may be raised. We will use the opportunity to demonstrate how use of forensic evidence can lead to better investigations that meet the threshold for information sharing with international partners.

All materials that require translation will be submitted to the Authority at the earliest opportunity (noting that due to Torchlight's previous deliveries of digital training, some of the material may already be available in Arabic). This will allow time for translation and printing of materials to be provided as 'handbooks' for the participants to serve as references guides that can be used as aide-memoires, post-delivery during day-to-day operations. A challenge in developing enduring technical capabilities is 'skill fade' due to limited or lack of use. As with most new technologies, it may take time for the demand to create the supply. To address this, the guides that we produce can be used as handbooks for operational use by the end users, providing a sustainable legacy of a 'leave behind' technical support that they can access at any time.

Our training approach is both conflict sensitive and gender sensitive—the materials will not include/condone any information that may go against our 'do no harm' strategy (as an example, we will not use case studies that may cause a divide culturally, religiously, etc amongst the trainees) and all the material will be gender neutral to enable delivery to a mixed gender audience.

As part of the training materials, we will also develop assessments. These assessments ('knowledge checks') will be based on the primary learning objectives for each of the training modules which are linked to the outputs described in our Theory of Change (see 1.2.8). There will be a minimum of two written assessments per module, combined with observations from our Delivery Team, providing a comparison of pre-course knowledge vs post course knowledge. This will be a key part of our data collection to inform our MERL. The assessments will enable continual monitoring and appraisals on the performance and knowledge retention of the participants. Practical sessions will also be carefully monitored and documented. The analysis of this data will be overseen by our Project Manager to maintain a level of impartiality from those collecting the information. These knowledge checks will enable us to collect documented evidence to support the MERL for this project.

Digital Evidence Training Course (estimated 5 days)

Delivered by our Digital Evidence Expert and CT Investigations Expert, the Digital Evidence module will provide awareness and understanding of digital evidence practices/procedures and develop competency in use of the equipment. The course outline will be tailored to the specific needs of the end users, with reference guides provided (see Output 6 below). A 'Prior Knowledge Check' and 'Knowledge Transfer Check' will be conducted to provide measurable evidence of the progression of participants. The course will enable participants to get hands on experience using the new equipment/tools, allowing time for mentoring by our team. Below is an indicative list of learning objectives taken from our 'Foundation' and 'Intermediate' level Digital Media exploitation courses that we would expect participants on this project to be able to do upon completion of our training (course materials from the 'Advanced' level course are also available from which our Trainers can draw upon):

Digital Evidence Training Course
Explain which types of evidential data can be obtained from which devices and the estimated time to obtain such data;
Understand the role of a Digital Media Examiner and how ISO 17025 plays an important part in consistent, repeatable, defendable approach to digital forensics investigations;
Explain the rules and requirements for the admissibility of digital evidence within local court proceedings;
Describe the technology available to a digital examiner and understand which tools are best suited to tasks;
Highlight Human Rights considerations of Right to Privacy, Collateral Intrusion inherent in digital data retrieval
Prepare a digital evidence log;
Triage and prioritise collation of digital evidential data;
Demonstrate competency in use of extraction tools;
Demonstrate the ability to verify and enrich evidential data;
Explain the evidential burden of proof, along with the individual steps recognised as international best practice (documented within the UK (NPCC) guidelines);
Provide and understanding of methods for contemporaneous note taking relating to Digital Media;
Explain/discuss presentation of digital evidence in court.
Describe a forensic strategy and how it impacts the examination;
Explain legal powers, safeguards and restrictions for accessing personal data including Human Rights principles of proportionality, necessity, legality and accountability PLAN

Online Investigations Training Course (estimated 3 days)

Delivered by our Digital Evidence Expert and CT Investigations Expert, the Online Investigations module will provide participants with the knowledge and skills required to successfully and securely conduct a range of open source intelligence (OSINT) activities. The course will be tailored to the specific needs of the end users, with reference guides provided. A 'Prior Knowledge Check' and 'Knowledge Transfer Check' will be conducted to provide measurable evidence of the progression of participants. The course will enable participants to get hands on experience using the new equipment/tools, allowing time for mentoring by our team. Below is an indicative list of learning objectives taken from our 'Basic Online Investigation' course we would expect participants on this project to be able to do upon completion of our training (course materials for the 'Intermediate' and 'Advanced' level courses are also available from which our Trainers can draw upon):

Online Investigations Training Course
Understand the uses of Open Source information;
Understand the need for personal and organizational security when conducting OSINT research;
Conduct complex internet searching using a range of methods;
Find archived information online;
Extract and use metadata of information found online;
Geolocate files and images using online mapping;
Identify the location and source of online images using a range of methods;
Search for and verify the identity of individuals online;
Understand how to gather information about social media platforms;
Understand attribution of open source;
Describe an OSINT activity and decision log as an audit trail of who accessed the information and why, when;
Use a range of security measures to perform the above tasks securely.
Highlight and describe Human Rights concerns and obligations applicable to Online Investigations

Seminar on Forensic Awareness - Digital Evidence (2 days)

A 2-day Forensic Awareness seminar will be delivered to increase the knowledge of key stakeholders within the criminal justice system on the how to utilise digital evidence. Our CT Prosecutions Expert will join the Training Team who will facilitate the seminar which will draw heavily on input/participation from the participants. In addition to presentations on how digital evidence is exploited, a series of syndicate activities will be run using mixed groups of prosecutors, judiciary, investigators and digital examiners—this will not only enable them to exchange ideas/perspectives/experience but also promote better interagency cooperation. We will case studies and where possible, encourage presentations from the participants, particularly to practice court room presentation skills. *Throughout the first two training modules, if any of the participants demonstrate potential to become trainers, they may be able to shadow and support our Delivery Team during the seminar.* Below is an indicative list of learning objectives we would expect participants on this project to be able to do upon completion of our training:

Forensic Awareness - Digital Evidence Seminar
Define the term ‘forensic evidence’ and describe types of evidence;
Describe types of digital evidence;
Understand use of open source in investigations;
Describe continuity of evidence;
Understand how attribution of digital evidence can be achieved;
Explain the rules and requirements for the admissibility of digital evidence within local court proceedings;
Describe and explain legal powers, authorisation processes required to acquire digital material, Human Rights obligations and compliance.

Output 6: Practical policies and tools to ensure strong management of capability, captured in a handbook to support application in day-to-day operations

Throughout the training modules, the Delivery Teams will work with the end users to develop policies, SOPs and the tools required to support the practical, legal and accountable use of the new capabilities. This will ensure that these are fully in line with existing policies/procedures whilst also meeting evidential requirements and standards (Output 6). A basic digital evidence management log will be introduced during the first module and it will be used throughout the training. It will be simple and easy to use but will contain information required for any case management system. It will provide a tracking system for all actions involving the evidence, showing step by step its receipt, exploitation, analysis and storage, as well as who was involved. This is a critical aspect to documenting how integrity of evidence was maintained and is a requirement of court for admissibility of evidence, it also provides HR safeguards by reducing the scope for evidence tampering, compromising the right to fair trial. The policies, SOPs and handbook will also provide guidance on Human Rights protections and assurance. The provision of this technical and tactical capability can lead to Human Rights concerns and breaches. The guidance will describe the legal parameters under which personal data can be accessed, processed, stored and shared and the authorisation processes and procedures required to access certain data.

Policies and SOPs will be captured in two Handbooks:

1. Technical management handbook – for systems administrators – how to back up, update, technical support, patch etc.
2. User handbook –to act as a pocket guide during operations.

In this way, we go well beyond providing ‘training handouts’, leaving behind a comprehensive set of materials which will be used by beneficiaries to guide their work, accelerating uptake of technology and securing long term sustainability.