APPROVALS BOARD PAPER 2 - CSIIF ASSESSMENT AND APPROVALS PROCESS OVERVIEW

APPROVALS BOARD CONSIDERATION

The 19 bids which passed the pre-assessment phase were substantively assessed based on a 0-100% weighted scoring mechanism as outlined below:

Section #	Details	Criteria	Weighting
1	Organisation Details	Due diligence	N/A
2	Initiative Description	Fit with policy - core criteria, additionality, diversity and inclusion	45%
3	Initiative Implementation, Delivery & Impact	Credible approach to delivery and confidence on impacts, scale and reach	40%
4	Initiative Finances	Financial management	15%

We assessed and scored each individual question based on a scale of ‘no confidence’ to ‘full confidence’ . The full criteria and marking guide was provided to the independent assessors, but the core criteria for applications is set out below:

- Provide clear evidence that initiatives are likely to **identify**, **train** and **place** candidates who have not been previously employed as cyber security professionals into cyber security employment that reflects the training and knowledge acquired through the initiative, within 12 months of initial funding.
- Demonstrate a realistic prospect of becoming **self sustainable** within 12 months of initial funding. As and when government funding ceases, confidence would be needed to assure DCMS that the removal of funding from this initiative would not affect the continued viability of the applicant organisation.

We also stated that the assessment process gives additional weighting to initiatives that demonstrate a detailed plan for, and a commitment to, placing women (making up at least 50% of initiative cohort) into cyber security roles. For example, this could include initiatives that help female returners to work who have been out of the labour market due to caring responsibilities.

Funding was split into pots and each application was assessed against the individual pot criteria set out below:

- Pot 1 (£250,000 - 500,000): **Large and/or scaled up initiatives -** based on a sound evidence base (may include successful pilot and proof of principle), will get over 50 candidates into cyber security roles within 12 months, has already engaged with more than three employers to place candidates and presents clear requirement for government funding.

- Pot 2 (£20,000 - 50,000): **New, creative and/or innovative initiatives -** will get up to 50 candidates into cyber security roles within 12 months, has already engaged/will engage with more than three employers with interest in placing candidates and presents clear requirement for government funding.

- Pot 3 (£75,000): **West Midlands based initiatives -** will get a minim of 30 candidates into penetration testing cyber security roles within 12 months, will focus on candidates who are living or show a demonstrable intention of moving to the West Midlands, and has already engaged with more than three employer who have expressed interested in placing candidates.

Based on the empirical scoring, we have developed a recommended shortlist of bids to fund (PAPER 3, ANNEX 1). There were also a number of near misses due to lower scoring and funding limitations. However, we believe there is value in asking these initiatives to provide an outline of how reduced funding could still be used to achieve CSIIF policy aims, as set out in PAPER 3 ANNEX 2. If agreed, this would allow us to make use of the majority, if not all, the pot of £**[redacted figure]**. We believe the empirical scoring gives us two larger initiatives that fit in with policy aims of funding a smaller number of bigger initiatives, rather than a larger number of smaller initiatives, and looking to increase the diversity and volume of candidates entering the cyber security profession.

QUESTION FOR THE APPROVALS BOARD

- **Based on the scoring and marking methodology, are you content that DCMS assessors have assessed and shortlisted the 19 eligible bids robustly and transparently?**