Due Diligence on Awarded Initiatives: Findings, Considerations and Approach

**To note, this is an extract from a larger document which reproduces all Hacker House material and omits any information relating only to other bids.*

Policy intent for sponsored Cyber Skills Immediate Impact Fund (CSIIF) initiatives

The CSIIF has been designed to use government investment to incentivise and encourage a broader range of industry-designed and led activity to deliver an immediate boost to numbers and diversity working in the cyber security profession.

Organisations, such as charities or training providers, bid for funding to deliver effective and sustainable approaches to help identify, train and place more adults into the cyber security profession. They will be required to demonstrate a clear requirement for government funding to help develop the concept or for a government contribution to grow or refocus a proven and successful existing model.

This Fund is part of the £1.9 billion National Cyber Security Programme to build a sustainable supply of home-grown cyber security professionals, and complements existing initiatives, like CyberFirst that help to boost the diversity of candidates entering the workforce.

Awarded funding

Organisation	**Funding awarded**
[CSIIF Applicant]	**£[redacted figure]**
[CSIIF Applicant]	**£[redacted figure]**
[CSIIF Applicant]	**£[redacted figure]**
Hacker House Ltd	£100,000

Summary of due diligence approach followed

This approach for the due diligence was developed alongside the DCMS Finance and Grants team and in consultation with EY/Atkins in February 2018. The process is outlined here **[link removed].** This approach is broken down into three levels of increasing scrutiny that ranges from ‘existing government suppliers’ to ‘non-government suppliers and non-regularly engaged stakeholders’.

For the due diligence process carried out as part of the expanded CSIIF initiative, three suppliers underwent due diligence (Type 3) for non-government suppliers and non-regularly engaged stakeholders’; **[CSIIF Applicant]**, **[CSIIF Applicant]** and Hacker House Ltd. The fourth organisation sponsored, **[CSIIF Applicant]**, is an existing government supplier (Type 1 due diligence) for the [redacted].

As set out in the Grant Standards, our aim is not to eliminate risk altogether but to understand and manage it more effectively. This document will provide a high level overview of the due diligence findings. For further detail, see here **[link removed]**.

Findings of due diligence checks and acknowledge of risks

[Redacted: commercially sensitive information in regards to other applicant(s)]

4. Hacker House Ltd

Due diligence checks on the legal entity and beneficial owners turned up no significant points of concern. We will request additional documents for our own audit purposes as part of the due diligence process, which includes certificates of incorporation and DBS checks for both project leads, but do not envisage this to cause significant concern.

Google checks turned up no concerns relating to sanctions, terrorist, PEP and negative news screening of both the organisation and individuals named on the initial application or as listed on Companies House.

The financial aspect of the due diligence process found that returns for the organisation have been filed a micro company, which was listed as dormant until 31 July 2016. In 2018, this company reported assets of £19,119 and liabilities of £715,176.

Risk: The primary risk for the Policy Team to consider is how this organisation with a significant difference between its assets and liabilities would would manage a government grant to deliver the outlined project requirement, without the entire company becoming dependant on the grant for its own commercial sustainability.

Mitigation and approach going forward

Given the nature of the CSIIF and the organisations it is likely to fund, the Policy Team accept that new organisations and start-ups will have inherently more risk when funding. This is as a result of the lack of an existing cyber security retraining ecosystem currently in both the UK and global market. As such, where possible, the Policy Team operates with flexibility and a high risk appetite to fund initiatives that fit with the policy aims of developing this market.

In order to provide challenge and ensure continued viability of organisations commercially, post-DCMS funding, we will take a range of approaches, depending on due diligence results, to ensure that all organisations are appropriately monitored.

The Policy Team acknowledges the risks as outlined by the due diligence process above, and have set out mitigating actions and approaches going forward below.

[Redacted: commercially sensitive information in regards to other applicant(s)]

4. Hacker House Ltd

The Policy Team acknowledged the financial risk of sponsoring this organisation to deliver this initiative. It was also noted that the initiative does not meet the 'immediate' aspect of CSIIF and DCMS funding will constitute the totality of project funding. However, the Policy Team noted the reputation of the two Directors within the industry and the ultimate agreement this initiatives may, in the longer term, provide an effective solution that identifies, trains and places candidates into cyber security roles.

The Policy Team confirmed with the BEIS State Aid team that our approach for full funding was within required rules and the appropriate documentation was include in the grant agreement.

The Policy Team also noted that the initial request for £273,000 presented too much of a risk for an initiative of this nature, after receiving a revised project plan for a reduced amount of funding, agreed to sponsor the initiative for a maximum value of £100,000. It was felt that this sum represented the right balance between an investment in a project that would have a positive impact of the UK cyber security retraining ecosystem and a level of risk that the team could confidently manage.

This organisation will be subject to increased grant management, specifically focused on managing payments on a monthly basis with explicit reporting required on exact fund spending breakdown. We will not 'pay in advance of need' more than a month ahead of requirement and only upon a clearly articulated business need. Each case for advanced payment will be considered by the Policy Team and required CSIIF SRO sign off. In the month following the advance payment the organisation must provide a full accounting of how the money has been spent to meet the grant objectives.

In addition, to provide further assurance, DCMS will review the grant deliverables and progress of the initiative after every monthly payment. Factors that will be taken into account include, where available, the progress of the initiative in identifying, training and placing talent into cyber security roles, as well as the development of the sustainability elements of the project to ensure viability post-DCMS funding.

Alongside monthly project monitoring and financial reviews, account returns will be requested for review by the Policy Team every month, with guidance from the Finance and Grants team to ensure the appropriate level of monitoring is taking place. The Policy Team will have to be satisfied that the funds are solely delivering the outcome of the sponsored project, but have not become an integral aspect of the overall business' finances and the removal of these funds would not result in the collapse of the organisation. If deemed appropriate by the DCMS CSIIF SRO, funding can be terminated.

Outcome: Initially, this organisation was partially approved. Upon review and subject to mitigation measures being approved, we recommend full approval for funding as mitigation takes into account a reduction in grant value to lessen the department's exposure, further/enhanced due diligence steps, and funding in tranches with enhanced monitoring as set out in Grant Standard Seven.

Initial reporting and monitoring information requirement for awarded initiatives:

Timeline: March 2019 - April 2020

1. Policy team audit of actual grant spend
2. Reporting requirements against policy aims and agreed grant milestones, capturing lessons learned for policy development
3. Site/office visit by Policy Team
4. Review of returns and accounts by Policy Team
5. CSIIF SRO informed of overall project delivery and financial progress

Company	**M**	**A**	**M**	**J**	**J**	**A**	**S**	**O**	**N**	**D**	**J**	**F**	**M**	**A**
[CSIIF Applicant]	-	-		-		-	-	-		-		-	-	-
[CSIIF Applicant]	-	-			-		-	-			-		-	-
[CSIIF Applicant]	-	-			-		-	-			-		-	-
Hacker House Ltd	3, 4, 5	1, 2, 4, 5	1, 2, 4, 5	1, 2, 3, 4, 5	1, 2, 4, 5	1, 2, 4, 5	1, 2, 3, 4, 5	1, 2, 4, 5	1, 2, 4, 5	1, 2, 3, 4, 5	1, 2, 4, 5	1, 2, 4, 5	1, 2, 3, 4, 5	1, 2, 4, 5