Upskill in Cyber Pilot Evaluation

Final Report

March 2023

Authors: Ecorys UK and Perspective Economics

Government Social Research

Contents

List of figures

List of tables

Executive Summary

The Upskill in Cyber Programme

The government contracted SANS to deliver the Cyber Security Adult Training pilot, marketed as Upskill in Cyber. The programme aimed to identify and rapidly upskill individuals for roles in cyber security, with students undertaking two SANS training courses (SEC275: Foundations and SEC401: Security Essentials[1]) and receiving soft skills development. The programme ran as a ten-week, virtual programme which opened for applications on 30th May 2022. Applications closed on 27th June 2022 and delivery began on 4th July 2022.

Participation

- 217 students participated in the programme, out of 223 individuals who were offered a place.
- The programme exceeded targets for:
    - registrations (1,876 against a target of 1,000)
    - suitable candidates progressing to selection (581 against a target of 250)
    - unique views on the programme website (82,352 against a target of 4,500)
    - applications received from individuals residing outside of London and the Southeast (63% against a target of 50%)
- The programme was below target for applications received from those identifying as female (27% against a target of 50%).
- [The majority of applicants reported that they identified as from an ethnic minority (56% against a target of 20%).]
- Outcomes and impact

The learning platform and content

- Students provided positive feedback on the learning platform and the content of the programme. Interviews suggested that students preferred the learning platform used for delivery of the SEC275 course.

Students' knowledge, skills, awareness, and interest

- Qualitative feedback suggested that participation in the programme accelerated some students' move into the cyber security sector.

[1] See Annex Five: Glossary for more information about course content.

- Survey data suggested that students reported significantly higher levels of cyber security knowledge, skills, awareness, and career awareness in cyber security after taking part in the Upskill in Cyber programme
- It was not possible to detect positive change in terms of their interest in further cyber security training and computing training, nor in pursuing computing careers. This may be due to small sample sizes and high baseline scores.
- At the time of reporting, 39 students had secured jobs in the cyber security sector which they mostly attributed to the programme, while others secured interviews (58), were applying for jobs, or were finishing their training (40).

Outcomes for employers

- Employers interviewed identified personal outcomes, including a sense of satisfaction from supporting people to get into the cyber industry and the opportunity to develop mentoring skills; and organisational outcomes which tended to focus on the opportunity to increase exposure as a cyber security employer and recruit a more diverse group of potential candidates.

Recommendations

- Recommendations to improve and increase applications include applying mutually exclusive categories of accepted, maybe, and declined applicants to reduce the time taken to select applicants; implementing a static recruitment window; and additional marketing and promotion aimed at targeting female applicants.
- Recommendations to further enhance programme delivery include considering additional support for employers looking to introduce entry level cyber roles; extending delivery timelines to allow students more time to complete both exams; and introducing more tailored support and guidance for career changers, as interviews suggest these students can face additional barriers to entering entry level positions.
- It is recommended that changes are made to future data collection to assess outcomes and impact in the longer term. It is suggested that one post-exam only survey is sufficient to gather the data needed to understand students' knowledge, awareness, and perceptions after the completion of the programme; and it is proposed that a follow-up survey 6 to 12 months after aimed at students completing the course could provide with further insight into the long-term impacts of the programme.

Introduction

In January 2022, the government commissioned Ecorys and Perspective Economics to evaluate the Cyber Skills Programme, consisting of the Cyber Explorers and the Adult Skills pilot. This report covers findings from the Adult Skills 'Upskill in Cyber' programme, drawing on feedback from students and employers participating in the programme, and data from Management Information (MI) provided by SANS (the delivery provider).

The Upskill in Cyber programme

The government contracted SANS to deliver the Cyber Security Adult Training pilot, marketed as Upskill in Cyber. The programme aimed to identify and rapidly upskill individuals for roles in cyber security, with students undertaking two SANS training courses (SEC275: Foundations and SEC401: Security Essentials) and receiving soft skills development. The programme ran as a ten-week, virtual programme which opened for applications on 30th May 2022. Applications closed on 27th June 2022 and delivery began on 4th July 2022.

As outlined in the invitation to tender, the focus of this intervention is to provide proof of principle that the talent pool for cyber security (which is currently limited and not diverse) can be grown through targeted intervention that brings individuals to a defined and easy-to-communicate aptitude. Thereafter, candidates should be meaningfully engaged with employers and offered a guaranteed interview on completion of the course.[2] The pilot aims to:

- Promote cyber security as an exciting and recognised career choice, with increased emphasis on candidates from underrepresented groups in the cyber profession, as well as those from lower socio-economic backgrounds.
- Provide a time-limited and effective skills boost for successful candidates that meets the needs of employers and is aligned to the baseline skills requirements required by organisations to implement the basic security requirements of the Cyber Essentials scheme.
- Engage employers in both design and delivery to encourage involvement and guarantee interviews with participants upon successful completion of the training solution.
- Deliver training solutions across the UK, with at least 4 different areas of the UK to be identified in order to support local individuals to benefit from this opportunity. SANS worked with government in the start-up phase of the programme to agree

[2] The KPI of all students achieving an invitation to interview was not in the original ITT, but was introduced during programme delivery.

appropriate geographical areas for the pilots (Greater London, the West Midlands, the Northwest, and Scotland).

The evaluation

The evaluation is being implemented by Ecorys and Perspective Economics. The following sections outline a brief overview of the evaluation strands and data collection achieved; the scope of this report; and the data limitations relating to the quantitative and qualitative findings. The full list of research questions is available in Annex Two.

Methodology

The evaluation takes a mixed methods approach involving both quantitative and qualitative data collection. The following table shows the various strands of data collection, and the sample sizes achieved for each as of 14 November 2022. A detailed overview of the methodology is provided in Annex One.

Table 1: Data collection

Data collection	Sample achieved (14/11/22)
Application and baseline survey data	1,876 applicants 217 accepted students
Interviews with students	37
Written feedback from students	6 follow-ups (from students previously interviewed) and 4 pieces of written feedback from students who were unable to attend interviews
Interviews with employers	5
Interviews with policy stakeholders	3
Follow-up student survey (post training)	45 (RR[3]=40%)
Follow-up student survey (post exam)	82 (RR=77%)
Follow-up student survey (post training and exam combined)	103[4] (RR=72%)
Matched pre-post sample (baseline accepted and combined follow-up)	103
Follow-up non-participant (declined applicant) survey	93 (RR=6%)

Reporting

This report draws on data from all sources noted in Table 1 and Management Information provided by SANS. This report aims to address the key research questions highlighted in the initial invitation to tender, a full list of which is available in Annex Two.

The analysis in this report provides government with a profile of Upskill in Cyber students (e.g., their demographic characteristics), including participant skills, knowledge, and views of cyber security before the start of the programme. This analysis includes

[3] RR refers to the survey response rate

[4] The combined total is made up of 21 respondents who completed only the post-training survey, 58 only completing the post-exam, and 24 respondents completing both (i.e., it is counting unique respondents, rather than unique responses). The response rate is calculated based on the 143 people invited to either or both surveys (103/143=72%).

descriptive statistics as well as sub-group analysis and significance testing where this was feasible and appropriate.

Data limitations

This section outlines in brief the main data limitations relating to the qualitative and quantitative findings.

The key data limitations relating to the quantitative findings are:

- **Self-reported outcomes and interpretation:** Outcomes data (behaviours, attitudes, knowledge, skills, etc,) is based on subjective, self-reported data rather than more objective data, such as a test score. This may lead to bias. For example, respondents might overestimate their knowledge prior to enrolling to the programme, as they are not aware of gaps in their knowledge until these are highlighted by taking part in the programme. However, the pre-post analysis did not find any unexpected results (for example knowledge decrease after the training due to an initial overestimation), suggesting that students were broadly reporting accurate outcome levels in the baseline survey. In addition, post data from the post-training survey and the post-exam survey were almost identical, suggesting that students had a good understanding of their own ability and awareness, before seeing the final exam scores[5].
- **Pre-post analysis may not robustly assess the impact[6] of the programme:** Pre-post analysis results should be interpreted with caution, as they may show early indications of impact, but the size of the impact is not necessarily accurate. For example, we observe the potential differences in pre and post outcome levels, but those differences are not necessarily and wholly attributable to the programme. Instead, there might be other time-varying factors affecting the outcome levels of respondents which are not controlled for. For example, students' knowledge of cyber security could be increasing at the same time as the training but by other external factors, causing us to overestimate the impact of the programme.
- **Small samples:** Small sample sizes can lead to biased results and should be interpreted with caution. Although the pre-post analysis makes use of a sample of 103 people (which is above the standard rule of thumb of 30 for a significance test), parts of the secondary analysis in this report makes use of smaller samples. This is mostly seen among a few secondary questions only asked in the post-training survey (n=45), or for example in breakdowns of smaller sub-groups in

[5] See Annex one for comparison table and Recommendations section

[6] The feasibility assessment (see Annex six) aims to answer whether and how a robust impact evaluation of the programme could be feasible.

certain questions. Such cases are highlighted throughout the report to advise caution when interpreting results.

- **Detecting marginal improvements when starting from high baseline levels:** In many cases, baseline levels reported by students have been already very high, which limits the opportunity to allow for changes to be seen. For example, students rating their interest in cyber security as 9 out of 10 in the baseline means that there is only a maximum of 1 point change that could be expected. In addition, a very large sample would be needed to detect very small changes (for example 1,000+ students) which is not available in this case. However, this is not necessarily a problem, as long as pre-post changes are moving in the right direction (for example an increase in knowledge levels), and those high baseline levels are maintained after the completion of the programme.
- **Incomplete post data:** At the time of writing, we are aware that many students are still completing their training and have scheduled exams for the end of November and December. As of 14th November 2022, 74 students had not yet received a post survey[7], and thus we do not have data on those students. In addition, certain longer-term outcomes for students are expected to materialise after the completion of the programme and the last cut-off point of our data collection. For example, the latest dataset shows that 39 students have secured jobs, but this is expected to increase further as remaining students attend interviews and provide updates on interview outcomes. The lack of complete post data poses a challenge in reporting accurate numbers as well as using those for the final VfM analysis.

The main limitation relating to the qualitative findings are:

- **Qualitative data does not reflect the prevalence of views**: interviews are used to illustrate the range of views held by students and employers and should not be interpreted as implying the prevalence of views among either group.
- **Interview timings**: For practical purposes and in order to capture early views of the programme, as discussed above, many interviews were conducted before students had completed training or attended job interviews so only early outcomes were captured.

[7] See Annex one: Methodology under Surveys for more details.

Programme participation

This section examines total participation numbers across the programme and diversity across key demographic characteristics, based on targets relating to gender, geographic spread of participation, and others. This section also draws on qualitative feedback from students and employers to discuss motivations for applying for Upskill in Cyber and views on the platform.

Applications

This section provides basic details on applications to the programme. This includes a review of the application and baseline survey data, in addition to qualitative findings regarding learner enrolment, participation, and sentiment.

Applications to the Upskill in Cyber programme in numbers

- 1,876 applications were received (87% over target)
- 581 suitable applicants (132% over target)
- 82,352 unique views on the programme website (1730% over target)
- 56% of applications received from those identifying as ethnic minorities (36 percentage points above target of 20%)
- 27% of applications received from those identifying as females (23 percentage points below target of 50%)
- 63% of applications received from individuals residing outside of London and the Southeast (exceeding target of 50%)
- 217 students recruited (out of 223 individuals offered a place in the programme, meaning an acceptance rate of 97%)

Overall, 223 places were offered, 217 of which accepted the offer and went on to participate in the training (1,649 or 88% of applications were declined, while the remaining less than 1% withdrew or declined their offer). The majority of declined applications (78%, n=1,649) were due to a low CyberTalent Enhanced Assessment (CTE) Score, while a fifth of those applications (20%) were declined due to training places already taken[8]. The remaining small minority (less than 2%) were declined due to their previous cyber qualifications (most holding a COMPTIA Security+ qualification) or

[8] The SANS selection process entailed a waiting period at the start of the applications, for average CTE scores to be estimated before starting to accept applicants. SANS accepted students starting from those with high aptitude scores and then those with lower scores evaluated on a case-by-case basis. After the 217 places were filled, SANS stopped accepting students regardless of their test scores.

current jobs in the sector. As expected, CTE scores among accepted applicants are significantly higher than those not accepted, as on average accepted participants scored 66 in CTE overall and 74 in CTE aptitude, while not accepted applicants scored 39 and 44 respectively. See Figure 2 for a full breakdown of the flow of candidates from application through to completion, or alternative outcomes as estimated from the non-participant survey.

Profile of applicants

In this section we outline findings regarding the profile of applicants to the Upskill in Cyber Programme. These findings are also meant to inform the feasibility of conducting an impact assessment of the programme[9].

Most applications came from individuals who identify as male (72%, n=1,876), while 27% identified as female. Although this was below the initial target (50%), we recognise that this was ambitious, as female representation in the technology sector, including cyber security, is still much lower than male. At the time of writing, 22% of the cyber workforce are female, meaning that the 27% female participation rate of the Upskill in Cyber programme is still above industry standards[10]. It was thus expected that the target of 50% might not be reached, although it was still deemed worthwhile setting such targets to motivate and improve female representation in cyber programmes.

Applicants were on average 36 years old. More than half of applications came from individuals identifying as ethnic minorities (55%, n=1,876), while the rest identified as individuals from white ethnic backgrounds (45%[11]).

The majority of applications came from England (88%, n=1,876), with smaller proportions coming from Scotland (7%), Wales (3%), and Northern Ireland (2%). Overall, most (63%) applications came from areas outside London and the Southeast, exceeding the KPI target of 50%, with 37% coming from London and the Southeast.

Most applicants (66%, n=1,876) were employed at the time of the application, with 89% of applicants having been employed in the last 5 years. A third of applicants (34%) were unemployed at the time of the application. Reasons behind unemployment were mixed, with the most common reasons being redundancy (17%), full-time education (16%), full-time parenting (10%), and illness/medical conditions (10%). Several applicants (41% selected 'other') mentioned Covid-19 related job cuts, limited-time contracts expiring, and

[9] See Annex six

[10] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf

[11] This includes "white: Irish" and "other white backgrounds."

actively seeking a new job or career change. This is explored in more detail in the following section about reasons for participation in the programme.

Currently employed applicants were working in a variety of different sectors, aligning with above findings regarding unemployed applicants looking for a career change, as well as the programme being open to individuals with no prior involvement/ knowledge in cyber. Common jobs among applicants were in information technology (12%), healthcare (12%), retail (8%), education (7%), transport and logistics (6%), hospitality and events management (6%), and public services and administration (5%, n=1,205). It is worth noting that the majority of currently employed applicants were working full-time jobs at the time of the application (72%, n=1,205).

In terms of education backgrounds, most applicants (71%, n=1,876) held qualifications beyond GCSE in England, Wales, and Northern Ireland, or beyond National 5 in Scotland.

Reasons for participation in Upskill in Cyber

This section draws on qualitative feedback from students who participated in the programme. Interviews suggested that, as anticipated, major themes in terms of motivations for applying included the opportunity to develop cyber security skills to move into a related career. Interviews suggested that students came from a range of employment and education backgrounds, some with previous computing or IT experience, some without.

Specific factors that encouraged students to apply for this programme compared to other programmes or opportunities included the government backing, which gave students confidence in the quality of the training and its relevance to industry; the flexible nature of programme delivery, which allowed students to complete the course at their chosen pace to accommodate work and family situations; and the fact that it was fully funded. With regards to funding, a major theme was that students would not have done that specific training course if they had to self-fund. Some students said they would have pursued training elsewhere, for example through free online courses or undertaking a computer science degree, while others suggested they would have stayed in their existing role and probably not developed those specific cyber security skills. Some students said they might have sought out alternative training courses, but they were not aware of any other free courses that covered such a range of topics and in particular, the opportunity to engage with employers.

Marketing campaign

A significant proportion of applicants found out about the Upskill in Cyber Programme from online sources, such as LinkedIn (14%), Facebook (12%), sans.org (7%), Reed

(6%), Instagram (4%), and Indeed (1%). Approximately 9% of applicants heard of the programme from family and friends, or other word of mouth (i.e., from work colleagues, employers, etc.)

Applicants were asked to rate the usefulness of the information reviewed prior to beginning the application. Materials such as brochures, flyers and information in key websites were available to applicants. The following table shows how applicants rated this information regarding their usefulness. Overall, applicants scored all the information materials highly (all above average with a minimum 7.7 out of 10) but found that the upskillcyber.co.uk webpage and the programme schedule were the most useful in providing relevant information. The SANS website was also rated similarly high at 8.1 out of 10, while the Upskill in Cyber Promotional Brochure and Flyer were rated relatively lower than the rest (7.9 and 7.7 out of 10 respectively). It is worth noting that a large proportion of applicants did not see the brochure and flyer at all (34% and 43% respectively), while the SANS website, the Upskill in Cyber website, and the Schedule were viewed by relatively more people (17%, 9%, and 14% of applicants did not see these respectively).[12]

Table 2: Usefulness of marketing materials according to applicants

Marketing materials	Mean score (out of 10)	Standard deviation	N
www.sans.org	8.1	2.1	1,563
www.upskillcyber.co.uk	8.2	2.0	1,707
Upskill in Cyber Programme Schedule	8.2	2.0	1,611
Upskill in Cyber Promotional Brochure	7.9	2.3	1,244
Upskill in Cyber Promotional Flyer	7.7	2.4	1,072

Source: Ecorys analysis of SANS data

A major theme from interviews with students was that students were not always familiar with the wider marketing campaign, for example because they had been sent the link to the online application directly by a colleague or friend or because they did not remember much about it at the time of interview. Mixed views were shared by those who had seen marketing materials. One minor theme was that students found it helpful that job adverts emphasised that applicants didn't need to have any background in IT or computing, and that encouraged some students to apply for the programme. Some reflected that since completing the programme, they felt it was more suitable to those from a computing background and that this could be better reflected in marketing materials.

[12] All applicants were required to apply via the online application form hosted on the Upskill in Cyber website.

Delivery approach

Most students selected the 'OnDemand' option (81%), as opposed to the 'LiveOnline' option (19%, n=217). All students reported they have access to a computer they can use for online training, and 98% (n=217) that their computer met the requirements needed for the Upskill in Cyber training courses. The remaining 2% reported that their computer needed more free space in their hard drive and a more powerful CPU[13]. Applicants were asked about their computer requirements to allow SANS to plan effectively for students requiring support in terms of hardware. Accepted students were then contacted and offered a laptop loan, some of whom accepted, while others made their own arrangements to obtain suitable equipment.

A major theme from interviews was that students appreciated the flexible delivery model of the programme as they felt it allowed them to fit their studying around professional and personal commitments. Some noted that there was a lot of content to get through in a relatively short period of time, which felt pressured and intense at times, but a major theme was that students felt supported by SANS and the expected time commitments were clear from the start. A major theme from interviews with students was that the SEC401 course covered more material than the SEC275 course, so they would have appreciated additional time to complete this course and the accompanying GSEC exam.

Student characteristics

In this section we outline the characteristics of accepted applicants, i.e., the 'students' enrolled in the programme. Students were compared against not accepted applicants, as this will help us better understand the profile of those selected to participate, as well as inform the feasibility of any potential impact analysis in the future[14]. The two groups of individuals were compared across key demographic characteristics, such as age, gender, and ethnicity, as shown in the below table.

Our analysis shows that the two groups are similar in terms of age (on average 36 years old), gender distribution (on average 72% males and 27% females), and regional distribution (based on area KPI, on average 63% individuals come from outside London and the South East). However, the groups differ in all other characteristics tested, namely ethnicity, target area, education, and employment status. Relatively more accepted applicants come from white ethnic backgrounds compared to not accepted applicants (73% and 40% respectively). There are also differences in education levels among the

[13] CPU (Central Processing Unit), i.e., the 'brain' of a computer allowing it to run programmes.

[14] The 'not accepted' cohort could act as a comparator group in an impact assessment of the programme, while the accepted (participants) will act as the 'treatment group'. Differences in the profiles of the two groups can provide with further insight in terms of the feasibility and appropriateness of specific methods of impact analysis, as well as advise whether there is a need to weight the two groups in order to improve comparisons. The analysis was key to inform the feasibility assessment of a future impact evaluation (see Annex six).

two groups, as relatively more accepted applicants have qualifications beyond GCSE (78%) compared to not accepted applicants (70%). Lastly, accepted and not accepted applicants are different in terms of their employment status, as relatively more accepted applicants tend to be employed (73%) compared to not accepted applicants (65%).

The following table outlines all comparisons made between the two groups, including the type of statistical significance test used for each comparison:

Table 3: Comparison of characteristics in accepted vs not accepted applicants

Characteristic	Accepted		Not Accepted		Statistically significant difference
	N	Mean/ Percentage	N	Mean/ Percentage	
Age	217	35	1659	36	No
Gender	217		1659		No
Female	53	24%	462	28%	
Male	161	74%	1184	71%	
Ethnicity	217		1659		Yes
Ethnic minorities	59	27%	989	60%	
White ethnicities	158	73%	670	40%	
Area	217		1659		No
London and Southeast	70	32%	632	38%	
Outside London and Southeast	147	68%	1027	62%	
Education	217		1659		Yes
No post-GCSE qualifications	48	22%	492	30%	
Post-GCSE qualifications	169	78%	1167	70%	
Employment status	217		1659		Yes
Unemployed	59	27%	579	35%	
Employed	158	73%	1080	65%	

Statistical significant differences between accepted and not accepted applicants are estimated at the 5% level.
Source: Ecorys analysis of SANS data

A major theme from interviews with employers was that the programme appeared to have attracted a diverse group of candidates in terms of gender, ethnicity, age, and professional experience and this was highlighted as a key positive aspect of the programme as it helped employers to access a diverse range of potential employees. One employer noted a particular improvement on the number of female candidates compared to similar events that they had attended in the past as part of other programmes. The same employer emphasised the enthusiasm of students they spoke to

at the careers fair and they were particularly pleased to see students who were retraining from non-cyber sectors.

> "I thought every single candidate we spoke to was excellent, and I could really see the passion for wanting to do it as well. And what was really good for me was [that] there was a particular candidate that was doing networks and then retrained, which is great. I think in 2022 if you want to go and retrain, then you should go and do something different, don't be stuck in the same thing." *Employer*

A minor theme was that a small number of candidates were perceived as being less motivated to be there. One employer suggested that this could be improved by placing more emphasis upon testing attitude as well as aptitude at the application stage. Another employer felt that there should be less emphasis on the aptitude test in order to attract a more diverse group of students.

> "Everyone is good at different areas and using that [aptitude test] cancels out a lot of good candidates that may be good in other areas." *Employer*

Employers suggested that a focus on cyber adjacent roles could help attract participants from an even greater range of professional backgrounds. A major theme was the importance of featuring females in promotional campaigns, as well as in programme activities such as panels and career events.

> "I think the power of seeing industry leaders who are women is important. There has been a lot of success in the past when the speaker lists have included women. It is also important to try and to dispel myths that all cyber roles are very technical, and that it is typically young white males spending all day behind the computer." *Employer*

Employer participation

Employers supported several elements of the programme, including virtual mentorship, soft skills sessions (for example CV writing), and the virtual careers fair (for example, answering questions from students about job roles at their company or joining an industry panel on themes such as threats and trends in the sector). Five employer interviews were completed as part of the evaluation. This section presents these employers' views of the programme, specifically their awareness of the programme, reasons for involvement and suggested changes.

Employers represented a range of organisation sizes including small, medium and large businesses as well as government departments. Employers worked in a range of sectors including information technology, finance, telecommunications, and the public sector. While interviewees represented a range of sectors, most employers worked within a cyber security team or department.

Awareness and initial perceptions of the programme

Employers who participated in interviews found out about the programme through LinkedIn or via previous involvement with SANS courses such as Cyber Discovery. The SANS team reported that employers who had previously supported similar programmes were informed about Upskill in Cyber, as well as graduates of those programmes who were likely to now be employed in a cyber security related role. A minor theme was that the programme would benefit from additional promotion among industry partners, as marketing budget was not allocated to industry recruitment. Some suggested that there could be more notice for employers – delays to the programme launch affected engagement with employers and their ability to support - and more emphasis on the benefits for industry using aides such as case studies or success stories to encourage more employers to take part. One employer suggested targeting organisations or individuals who have entered the cyber security sector from a different professional background could help to attract more industry support. Another employer noted that investing in a targeted campaign could be effective, particularly in raising awareness of cyber adjacent roles.

Employers were asked about what they first thought about the programme when they found out about it. All interviewees expressed that they had very positive impressions of the programme and a major theme was that SANS' reputation was a significant factor in wanting to support the programme. One interviewee felt very encouraged that the programme was targeting adults, and those wanting to undertake a career change.

> "I think it is great that they [government & SANS] are targeting adults, because it helps the pipeline for those mid and senior positions and supports those people who want to career change rather than people who are coming straight into it at entry level." *Employer*

Some interviewees had worked with universities and other course providers such as CodeClan[15] and QA[16] in similar ways and others were aware of similar programmes such as CyberCenturian[17].

Employers felt that the Upskill in Cyber programme content was relevant for getting into the industry and understanding the fundamentals. Most interviewees were aware of both

[15] https://codeclan.com/
[16] https://www.qa.com/
[17] https://cybersecuritychallenge.org.uk/what-we-do/cybercenturion

the GFACT and GSEC qualifications however there were mixed opinions on their importance. A major theme from interviews with those who were aware of the GFACT and GSEC was that they were good foundation qualifications and offered an indication of a baseline of cyber awareness. Where the interviewees compared the GFACT and the GSEC, they felt that the GFACT held more weight. A minor theme was that although the GFACT and GSEC isn't something that specific employer would require in an applicant, it is one of a number of certifications that they find desirable and they would feel confident that a candidate with those certificates had the necessary level of knowledge and skills.

Reasons for involvement

Employers were motivated to take part in the programme by the opportunity to recruit candidates into their respective organisations, gain access to a diverse pool of talent and to give back and support people to get into the industry.

The opportunity to recruit potential candidates for cyber security roles emerged as a major theme across all interviews and employers emphasised that this was particularly attractive at a time when it is difficult to hire in the industry due to a shortage of skills. Employers felt that the Upskill in Cyber programme was particularly attractive because of the diversity of programme participants, which aligned with their organisations' aims to increase diversity within their cyber security departments.

> "[If I didn't take part in the programme] I would need to put a lot of effort in networking with multiple universities and organisations whereas this programme already has a really diverse pool of applicants from a range of different backgrounds, genders and ethnicities." *Employer*

Secondary factors included the opportunity to give back to the sector by helping to upskill the next generation of cyber security professionals, support people getting into the industry and provide mentorship.

> "The main thing is supporting this [the programme] and getting more people into the industry. We went into this knowing we might not get anyone, but if we do that's great as well." *Employer*

A minor theme identified by a small business was that they were motivated by the fact they were able to get involved for free, particularly as time commitments were flexible and events were held virtually.

Recommendations

Additional support for employers

Some employers suggested that they would like to see more support and guidance for employers looking to recruit for entry level roles. They suggested that SANS could work

with organisations to help them understand how to attract a diverse range of candidates and support and upskill those with lower levels of experience. They also suggested that a similar programme for non-technical roles, such as risk, auditing and governance could help to address skills gaps in those fields.

Additional support for participants

Some employers felt that participants would benefit from additional support for entering a career in cyber security, as they recognised that it can be a challenge to have a clear career path, particularly when coming from a background unrelated to cyber. One employer suggested making a resource for participants which maps out all the professions within cyber security and adjacent sectors to help participants decide on their next steps after completing the Upskill in Cyber programme. The employer thought something similar to the career route map created by UKCSC[18] would be useful, with the addition of the skill sets required for each route[19]. The interviewee felt that a career map, alongside a session on transferrable skills would be particularly helpful for candidates that were not sure how to utilise their transferable skills from previous job roles.

> "A lot of candidates were not aware of how valuable their transferable skills from their previous career experience were. They are really great, maybe they need some support with understanding what skillset they have and how it can be used in cyber roles." *Employer*

Another employer felt that participants would benefit from signposting towards additional training and qualifications to help them in their career path.

Candidate profiles

One employer said they would have found it helpful to receive candidate profiles, including their aptitude test scores. They felt it would have been useful to know candidate backgrounds including their experience and strengths to assist them in recruitment activity.

[18] https://www.ukcybersecuritycouncil.org.uk/qualifications-and-careers/careers-route-map/

[19] This particular interviewee was unfamiliar with the SANS Cyber Security Skills Roadmap: https://www.sans.org/cyber-security-skills-roadmap/

Outcomes and impact

Summary

- Qualitative feedback suggested that students found the application process efficient and straightforward. A minor theme was that some students felt that applicants with a background in STEM subjects or computing had an advantage in the aptitude test.
- Students provided positive feedback on the learning platform and the content of the programme. Interviews suggested that students preferred the learning platform used for delivery of the SEC275 course.
- Survey data suggested that students reported significantly higher levels of cyber security knowledge, skills, awareness, and career awareness in cyber security after taking part in the Upskill in Cyber programme
- It was not possible to detect positive change in terms of their interest in further cyber security training and computing training, nor in pursuing computing careers. This may be due to small sample sizes and high baseline scores.
- At the time of reporting, 39 students had secured roles in the cyber security sector and a further 58 students were awaiting interview outcome.
- Employers interviewed identified personal outcomes, including a sense of satisfaction from supporting people to get into the cyber industry and the opportunity to develop mentoring skills; and organisational outcomes which tended to focus on the opportunity to increase exposure as a cyber security employer and recruit a more diverse group of potential candidates.

Recommendations relating to programme delivery

- Consider additional support for employers looking to introduce entry level roles to their organisation.
- Extend delivery timelines to allow students more time to complete both exams
- More tailored support and guidance for career changers, as interviews suggest these students can face additional barriers to entering entry level positions.

Recommendations relating to data collection

- It is suggested that one post-exam only survey is sufficient to gather the data needed to understand students' knowledge, awareness and perceptions after the completion of the programme.
- We suggest that a follow-up survey 6 to 12 months after aimed at students completing the course could provide with further insight into the long-term impacts of the programme.

This section covers students' knowledge, skills, awareness, and interest relating to cyber security and related careers. It draws on the student baseline and post surveys and

interviews with students and employers. This section presents changes over time on students' and employers' perceptions of the platform and early outcomes for students.

Views on the application process

Major themes from interviews with students were that the application process was straightforward, and that the aptitude test was difficult, but seen as an effective and suitable way of identifying the best candidates for the programme. Some students noted that the aptitude test provided useful insight into content that might be covered on the course. Some students said they felt that a background in STEM subjects or computing helped them to achieve a high score in the aptitude test, and they wondered whether applicants without that background would struggle to understand the questions and what was required. Students perceived the aptitude test as testing their mindset and ability to take initiative, rather than testing their technical knowledge, although a minor theme was that students found the questions to have more of a technical focus than they were expecting considering the course was advertised as not requiring any background in computing. A further major theme was that students would have appreciated feedback on the aptitude test to help them identify areas of strength and weakness.[20]

Views on the learning platform and content

Overall, students provided **very positive feedback on the learning platform and content of the training**. The follow-up surveys suggested that students found the programme beneficial as almost all students (98%, n=82) said it was extremely likely (76%) or likely (22%) they would recommend the programme to a friend. Most students found the two learning courses enjoyable, although students appeared to have enjoyed the first course more than the second, possibly due to the advanced difficulty. Most students (87%, n=45) said the SEC275 course was very enjoyable (49%) or enjoyable (38%), while a lower majority of students (62%) said the SEC401 course on security essentials was very enjoyable (22%) or enjoyable (40%). A major theme from interviews with students was that they preferred the delivery style of SEC275, for example they found the lecturer easier to follow and appreciated the availability of written transcripts[21], although it was recognised that this may relate to different learning styles.

In terms of the ease of use of the available platforms, students also had positive feedback. Students found the SANS portal (the learning platform) easy to use for the training, as 47% reported it was "very easy", 38% said it was "easy", while the rest (less

[20] CTE results are not shared with applicants to the programme. As the CTE tool is used across multiple programmes delivered by SANS, providing feedback on applicant performance could reveal SANS selection measures and therefore impact recruitment of future programmes.

[21] Printed and digital course materials were made available for both courses.

than 10 people[22]) felt neutral or that it was difficult to use (n=45). Students also found the GIAC portal (used for the exam) easy to use as well, as 38% said it was “very easy”, 44% said it was “easy”, while the rest 13% felt neutral and 5% that it was difficult to use (n=82). A major theme from interviews with students was that students preferred the platform used for SEC275 as it was reported to be more user-friendly, compared to the SEC401 platform which was perceived as outdated.[23]

The majority of students (80%) were also satisfied (35%) or very satisfied (45%) with the exam environment (n=82). Most students chose to do the exam remotely (56%), while the rest went to a test centre (44%, n=82), while this did not seem to affect the satisfaction of students regarding the exam environment. Interviews suggested that students appreciated the flexibility of exam options and any minor issues relating to booking or taking exams were dealt with quickly with support from the SANS team.

In terms of the difficulty of the two courses and exams, responses were mixed, suggesting a variety in the level of abilities, skills, and confidence among students. Students reported mixed views in terms of reported difficulty of SEC275, as 42% found it difficult, 31% found it neutral, and 24% found it easy (n=45). However, most students (76%) found SEC401 difficult (51%) or very difficult (24%), which was expected as it is a more advanced course meant to challenge students (n=45).

Aligning with the above results, students overall had mixed views but found the GSEC exam to be more difficult than the GFACT one, which is again expected due to the advanced level of content. Students reported mixed results in terms of reported difficulty of the GFACT exam, as 37% found it neutral, 28% found it easy and 22% found it difficult (n=82). However, students found the GSEC exam to be more difficult, as 51% said it was difficult, 27% found it neutral, and 12% found it easy (n=82).

It is worth noting that students overall felt well equipped to face the exam, as they scored 7.6 out of 10 (n=45) in terms of their preparedness (a score with 1 being not at all equipped and 10 being extremely equipped). This is also reflected on the results of both

[22] As sample sizes are relatively small, we do not report low percentages or numbers to avoid identification of respondents.

[23] SEC275 is delivered via a dedicated platform, which contains the written, visual, and audio content required to study the course, as well as the interactive labs used to embed learning and practice technical concepts. The interactive labs can be completed within the web browser and no additional software is required. For the SEC401 course, participants who did not opt to study via the LiveOnline method studied via SANS’ OnDemand method, which is embedded within www.sans.org. The OnDemand platform consists of pre-recorded video lectures from a SANS Instructor, as well as end of module quizzes. During the delivery of Upskill in Cyber, SANS rolled out an updated version of the OnDemand platform. The new player was designed in response to student feedback and includes a modernised interface with improved accessibility, easy to access help and support, an improved layout for the course outline, course notes, and search, as well as prominent course progress information allowing users to monitor progression.

exams, as most students passed. At the time of reporting (14th November 22) 149 students (69%, n=217) have completed both courses. More students are expected to take exams within November and December 2022, thus these numbers are expected to go up. These findings, alongside students' high levels of enjoyment could suggest that the level of difficulty of the training courses and exams was viewed positively by students as they engaged and gained significant knowledge and skills along the way.

Interviews suggested that overall, students were satisfied with programme delivery and content. No suggestions for additional topics were made and some students said the programme exceeded their expectations in terms of diversity of content and quality of training.

> "I've learnt more in 5 weeks than any college I've been to. Doing it all in five weeks really impressed me. I'd tell people to do this course over college. Good content, adequate to a whole year of college." *Student*

> "I've been blown away actually at the breath and the depth of the information contained within the courses. I almost think that calling it 'foundational cybersecurity technologies and security essentials' does it a disservice as to how in-depth it is because there are a lot of other [courses] out there that are called foundational or entry level and this was worlds apart in terms of the content and what we were expected to learn." *Student*

A major theme from interviews with students was that the programme was rated highly in comparison to other course or initiatives which students had taken part in, in terms of breadth of content and relevance to industry.

> "It blows the socks off any other courses. Above and beyond. The fact it's constantly kept up to date…I just had a conversation today about some StackSocial pen testing courses. I'm sat in an office with people who went to university, and they feel that things they've been taught are out of date. When some of them were at university, cloud computing wasn't in the curriculum. The fact [this course] is kept up to date is phenomenal." *Student*

Views on wider support from SANS

A major theme from student interviews was that students praised the level of support provided by the SANS team, noting that they were highly approachable, easy to get in touch with through a variety of mechanisms, including the Slack channel and email, and

the team responded quickly to any queries. Some expressed gratitude to the SANS team for allowing them extensions when needed and noted that this alleviated stress.

Students and employers who had taken part in soft skills sessions or the careers fair reported that these were valuable in helping them to prepare for applying for jobs and attending interviews. A major theme was that many sessions were perceived by students as being more relevant and useful for early career students with more limited experience of preparing CVs and attending interviews. A minor theme was that it would have been useful for more of the soft skills sessions and events to be held during evenings or weekends[24], to accommodate students who were working full time, although it was noted that recordings were available, so students were able to catch up in their own time.

Employers provided positive feedback on the careers fair, with a major theme that the event was beneficial as students were motivated to speak to employers about mentoring or about materials they had shared. Compared to other virtual careers fairs they had attended previously, some employers said they found it to be a more valuable use of time as there was a clear purpose.

> "Everyone you spoke to was a potential employee." *Employer*

Other employers described the success of the drop in booth, which they felt gave their organisation a lot of exposure that they wouldn't have had otherwise.

> "We loved the drop in booth, that was really clever. We were talking to people all day." *Employer*

Students highlighted the availability of practice assessments as helping them to prepare for exams, as well as wider support from mentors and other students via slack channels. Some students noted that completing a practice assessment reassured them that they knew more than they thought, which built their confidence before undertaking their exam.

> "I go into panic mode when I go into exams. I think I was the best prepared that I could have been. It was mainly due to the peers and the mentors coming in with the indexes that we had to build for the exam. I've never heard of indexing before…I think that was one of the main things in the course that really, really helped." *Student*

A major theme was that students appreciated the flexibility in terms of mechanisms to ask questions and seek support from lecturers and SANS staff. For example, some reported feeling shy about asking questions on public channels, and said they preferred to message lecturers directly. Some students and employers suggested they would like

[24] Four of the six soft skills sessions were delivering during weekday evenings. Two were delivered during normal business hours.

to see 1:1 bookable slots with employers made available at the careers fair, as some students did not feel comfortable talking and asking questions in a group environment.

> "I did think that the booth environment may not be the most accessible for someone who is neurodivergent because they may not feel comfortable in that environment. They may feel more comfortable with a one-to-one chat." *Employer*

Employers highlighted the mentoring aspect of the programme, as an effective way to support students. Some noted that the Slack channel meant they were able to get involved flexibly, at any time that suited them, rather than being restricted to work hours. They saw this as a positive aspect, as they were able to provide more immediate responses to students which kept discussions going.

> "I think the mentorship aspects, being able to share different perspectives and give people a better idea of the industry... I think that's a great aspect of the program." *Employer*

One employer noted that they felt they could have gotten more out of the mentoring if it had been more structured, for example through more targeted matching of students and mentors based on interests and background.

Some employers suggested that the career support element of the programme could place a larger emphasis on a wider variety of cyber and cyber adjacent roles. This is because they felt that when it came to the careers fair, most candidates were only aware of more common roles such as SOC analyst roles.

> "From what I could see on the slack and the mentorship channels, all I could see is that people were kind of expecting SOC analyst roles and not much else. But I think maybe we would have been good to touch on the breadth of careers in cyber." *Employer*

Knowledge, skills, awareness, and interest

Applicants were asked to rate their self-perceived knowledge, skills, awareness, and interest around cyber security, relevant careers, and broader computing skills. In this section we report on the responses of accepted applicants before and after taking part in the Upskill in Cyber Programme (n=103) as well as qualitative feedback from students and employers. A pre-post analysis[25] was conducted to identify whether there were differences in the perceptions, attitudes, and behaviours of participants due to their

[25] Pre and post survey responses were compared with a paired t-test, to assess whether differences are statistically significant.

participation in the Upskill in Cyber Programme. It is worth noting here that pre-post analysis results below should be interpreted with caution as they show changes over time, but not necessarily the true impact of the programme (see Data limitations section).

Overall, students have reported **significantly higher levels of cyber security knowledge, skills, awareness, and career awareness in cyber security.** Students reported an average change of almost 1 level (0.9), which translates to an increase from a basic level to intermediate or from intermediate to advanced. Students also reported a significant, although smaller increase (0.5) in their knowledge and skills about computing in general.

The following table shows in more detail the change in knowledge, skills, and awareness of Upskill in Cyber participants after they engaged with the learning content:

Table 4: Cyber security knowledge, skills and awareness

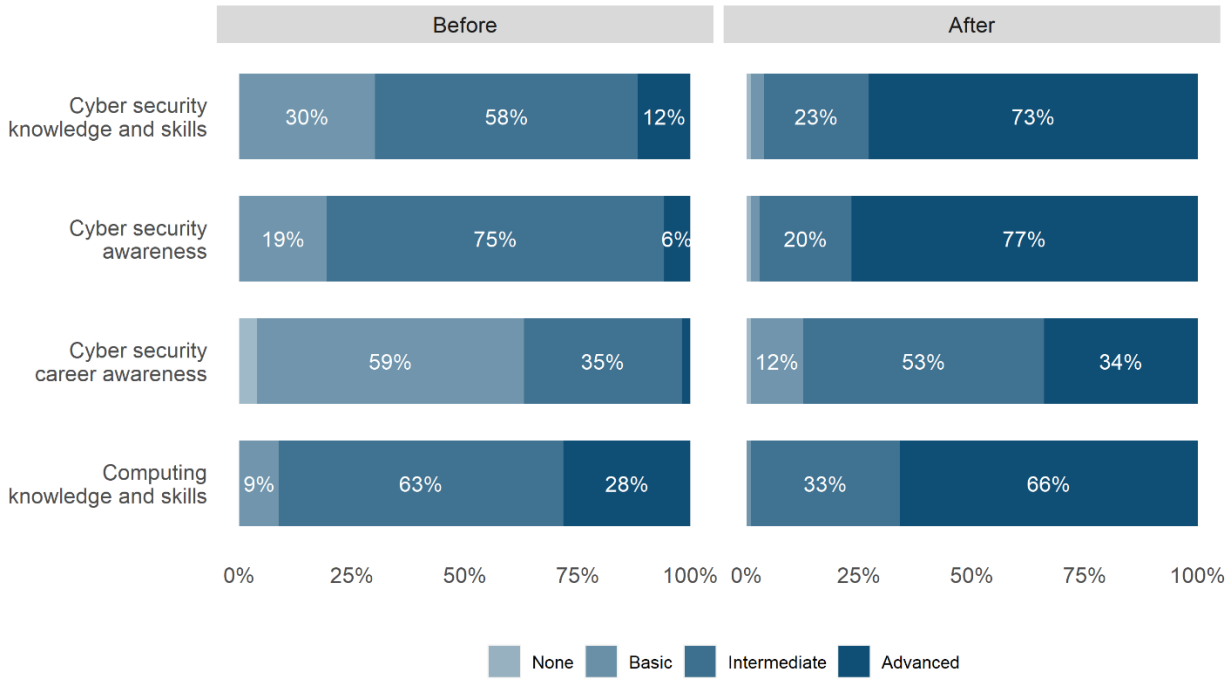
Survey question (n=103)	Before	After	Difference
Cyber security knowledge and skills	1.8	2.7	0.9*
Cyber security awareness	1.9	2.7	0.9*
Cyber security career awareness	1.3	2.2	0.9*
Computing knowledge and skills	2.2	2.7	0.5*

Source: Ecorys analysis of SANS data
Indicators in the table are scores of 0-3, with 0=None, 1=Basic, 2=Intermediate, and 3=Advanced.
The symbol '' marks if a difference between before and after means is statistically significant at the 5% level.*

After taking part in the Upskill in Cyber programme, **most students (73%) reported advanced levels of cyber security knowledge and skills**, compared to a much lower 12% before taking part. Similarly, **most students (77%) reported advanced levels of awareness about cyber security** after participating in the programme, compared to a 6% before participating. In terms of cyber security careers awareness, most students reported intermediate (53%) and advanced (34%) levels after taking part, compared to much lower proportions reporting intermediate (35%) and advanced (2%) levels before participating in the learning. It is worth noting that before the start of the programme, the majority of students (59%) were reporting basic levels of awareness, while this is the minority after taking part (12%). This, alongside above findings, suggests that **students' awareness about cyber security was significantly increased** during the course of the programme. Lastly, students also reported higher levels of computing knowledge and skills, as most (66%) reported advanced levels, compared to 28% before participating in the programme. It is worth noting that there are almost no students (less than 10) reporting basic levels of computing after taking part (compared to an initial 9%), as almost all of them are reporting advanced and intermediate levels.

The following graph outlines the average responses of students regarding their knowledge, skills, and awareness, before and after taking part in the programme:

Figure 1: Students knowledge, skills and awareness before and after Upskill in Cyber (n=103)



Source: Ecorys analysis of SANS data
Note: Percentages smaller than 4% are not labelled as the bars are too small to fit text

A major theme from interviews with students was that students felt their knowledge and skills relating to cyber security had significantly improved, and that the course exceeded their expectations in terms of what they gained from taking part in the programme.

> "I have gained experience, confidence, and a new perspective on the industry. As someone going into it thinking I already had a good understanding, that understanding has improved massively." *Student*

Students reported that they may have developed some of that knowledge and skills elsewhere, for example through pursuing alternative training courses, but a strong theme was that the programme accelerated students' learning and transition into a career in cyber security.

> "I potentially might have developed the same knowledge, but it would have taken ten times longer." *Student*

As part of the application process and baseline survey, participants were also asked to rate their levels of interest in training and pursuing careers in the cyber security and computing sector. Overall, **students reported significantly higher levels of interest in cyber careers** after participating in the programme compared to their initial levels of interest. Students rated their interest in cyber security careers at 9.2 out of 10, a change

of 0.6 points from their previous score of 8.5 out of 10 before the start of the programme (n=103). This was also their highest score compared to their interest in further training in cyber security and computing or in computing careers.

However, **no change was detected in terms of their interest in further cyber security training and computing training, nor in pursuing computing careers.** It is worth noting however that their initial levels of interest were already very high (almost 9 out of 10), and their levels after participating appear slightly higher (but not statistically significant). As these are very small changes at already high levels, it is possible that we are not able to detect statistical significance due to a relatively small sample. Interviews suggested that some students were planning to undertake further cyber security training after completing Upskill in Cyber, before applying for jobs, in order to specialise in a particular field of cyber security. In some cases, students reported that this had been their intention when starting the programme, again suggesting that there were high levels of interest at baseline level.

The following table outlines the average levels of interest in cyber security careers, computing careers, and further training in cyber security and computing, before and after taking part in the programme:

Table 5: Students' interest in cyber security and computing

Survey question	Before	After	Difference
Cyber security career interest (n=103)	8.5	9.2	0.6*
Cyber security training interest (n=102)	8.7	9.1	0.4
Computing career interest (n=102)	8.5	8.7	0.1
Computing training interest (n=102)	8.6	8.8	0.3

Source: Ecorys analysis of SANS data
Indicators in this table are scores of 0-10, with 0 being not at all interested, 5 being somewhat interested, and 10 being extremely interested.
The symbol '' marks if a difference between before and after means is statistically significant at the 5% level.*

Lastly, participants were asked several questions specific to cyber security careers, their confidence around pursuing such jobs and the level of knowledge/support they receive around the subject. On average, **students' knowledge and confidence around careers significantly increased after taking part in the programme**. Students are more knowledgeable and confident about the steps, skills, and qualifications needed to pursue a career in cyber security, as well as knowing where to find the right information and being confident enough to start working in a cyber security role. As shown in the table below, there was an increase of 1 point in almost all the below indicators (scale of 1-5), with the biggest increases identified in their knowledge of steps needed to pursue a cyber security career and knowledge of skills needed to pursue such careers (both increases of 0.9), and knowledge of qualifications needed to pursue a career in cyber security (1 point increase).

The table below shows in more detail how participants responded on average before and after taking part in Upskill in Cyber:

Table 6: Students' knowledge and confidence regarding cyber security careers

Survey question (n=103)	Before	After	Difference
Knowledge of steps needed to pursue a career in cyber security	3.3	4.2	0.9*
Knowledge of skills needed to pursue a career in cyber security	3.3	4.2	0.9*
Knowledge of qualifications needed to pursue a career in cyber security	3.0	4.0	1*
Knowledge of where to get information about pursuing a career in cyber security	3.5	4.0	0.5*
Confidence of being ready to work in a cyber security role	3.2	4.0	0.8*
Understanding of career pathways available in cybersecurity	3.2	4.0	0.8*
Lack of sufficient knowledge about cyber security in general to know if it is a career option	2.2	2.0	-0.2

Source: Ecorys analysis of SANS data
Indicators in this table are scores of 1-5, with 1=Strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, and 5=Strongly agree.
The symbol '' marks if a difference between before and after means is statistically significant at the 5% level.*

As described in the above section, 'Views on wider support from SANS,' interviews highlighted the value of additional career focused elements of the programme, such as the careers fair, mentoring and soft skills sessions in raising awareness of the diversity of cyber security roles and possible routes into the sector.

Students rated the programme very positively at **8.1 out of 10 (n=103) in terms of how helpful it was to position them for a career in cyber** (a score of 1 being not at all helpful and 10 being extremely helpful). At the time of reporting, (14th November 2022) 39 students had been offered jobs in the cyber security sector. This is expected to increase as more students complete their exams and provide updates on interview outcomes. The latest data showed that students attributed most of that to the programme (attribution score was 8.5 out of 10). It is worth noting however that the sample is very low on this as it was based on eight students who had secured roles at the time of completing the survey, so attribution to the programme should be interpreted with caution. In addition, 27% have been selected for an interview at a relevant role. As noted above, these proportions are expected to change as more students secure jobs and interviews after the final cut-off in our data (14th November 2022).

Interviews with students and policy stakeholders suggested there might be more students securing jobs and applying for roles in cyber security after the last data collection point thus a follow-up is advisable to gather more information (see recommendations section).

A major theme from interviews with students was that students found the programme valuable in raising awareness of career pathways in cyber security and preparing them to pursue a job in the sector. Some students had already been offered cyber security roles, while others were in the process of applying and felt confident that having these qualifications would help them to secure a role.

> “I've achieved career changing certifications that have definitely helped me get a new job in cyber security. And I also have foundational knowledge that’s going to be help me in my job” *Student*

> “What it gives you in the 8-10 weeks is very good. It gives you skills where you could go into a workplace and add value straight away, rather than just being a piece of paper.” *Student*

A further strong theme was that after completing the programme, students felt more motivated to pursue a career in cyber security. Students identified a range of factors which led to increased motivation, including a sense of satisfaction at being able to pass both exams, support from peers on the programme, and exposure to employers.

> “[I’ve gained] a massively increased motivation to make a career change, lots of new skills and information, and certainly some new ideas. I've made some new colleagues and acquaintances. It's definitely given me a network and good foundation on which to build a career from going forward. I’m still looking for a job at the moment but I'm sure that will come with time. Definitely a strong foundation has been built and I just found it extremely valuable.” *Student*

> “I would say joining this program has given me a fresh new mindset to go and try to create a new career. I see I'm one of maybe 150 others… trying to get this done and that's support enough to say that it is possible. You could see people posting [on Slack] all the time that they've got a job, they've changed jobs, they've got a new position. That's motivating to know that there are people who are going to give you a chance. And thanks to this course, you are at a kind of advantage.” *Student*

A major theme from interviews of students who were career changers, was that the programme helped them to understand the relevance of transferable skills, and how they could be applied to a job in cyber security.

> "Being able to get support on finding a job has been really helpful. I am probably going to go into a role of writing training materials which will link in with my degree [in creative writing]. The careers people that there were like, 'Oh you do creative writing and cyber stuff. We're dying for people like you to write training materials'". *Student*

Interviews with employers suggested that employers felt confident that the programme was beneficial for participants. Employers noted that the attainment of two reputable SANS qualifications would have equipped students with the skills and knowledge required to enter the cyber security job market. A major theme was that the additional support, such as the careers fair and soft skills sessions, provided students with opportunities to build networks with cyber security employers and led to a greater awareness of jobs and career paths in cyber security.

Participants were also asked which elements of cyber security upskilling programmes they deem the most important (in a 4-point scale from "not at all important" to "very important"). **Students rated training delivered by a reputable provider as the most important factor for upskill programmes** after completing the training, closely followed by **technical content, flexibility of learning method** and **industry recognised certifications/qualifications**. Students' perceptions about which aspects are important are generally consistent before and after the programme, as there are only a few changes identified which are relatively small in size. It is worth noting that, as above, many of these aspects were rated very highly at the start of the programme. Therefore we cannot expect to be able to detect very small or large changes. For example, many aspects were already rated at 3.8 out of 4 in importance, meaning that a maximum change of only 0.2 would be possible.

Students attributed **higher levels of importance** (compared to the baseline) to the **flexibility of learning methods, the flexibility to learn at one's own pace, low fees, and government backing.** However, Students attributed **lower levels of importance** (compared to the baseline) to opportunities to engage with industry/potential employers, access to Teaching Assistants/Subject Matter Experts to aid learning, and soft skills content (e.g., communication, teamwork). As noted in the 'views on additional support' section, soft skills sessions were perceived as most useful and relevant for less experienced students compared to those with existing careers who reported already feeling confident in aspects such as preparing CVs and interviewing.

Students ranked face-to-face training delivery as the least important aspect of upskill programmes, which they reported consistently in the baseline and follow-up

surveys. This is not surprising considering the delivery method of the programme itself, as well as current trends towards remote learning. Lastly, the majority of students reported that financial support is also important in upskill programmes (95% overall; 65% rated very important, 30% rated quite important, n=103). It is worth noting that this was asked only in the post surveys, thus we are not able to compare whether perceptions have changed over time in this particular subject. However, as mentioned above, students rated low fees as an important aspect of upskill programmes, which they rated even higher after taking part in the programme.

The following table shows in more detail how participants of Upskill in Cyber rated aspects of such programmes, before and after taking part:

Table 7: Important aspects of upskill programmes as reported by participants

Survey question (n=103)	Before	After	Difference
Training delivered by a reputable provider	3.7	3.8	0.1
Technical cyber security skills content	3.8	3.8	0.0
Flexibility of learning method	3.6	3.8	0.2*
Industry recognised certifications / qualifications	3.7	3.8	0.0
Access to remote learning	3.7	3.8	0.0
Quality of Instructors	3.8	3.7	0.0
Flexibility to learn at your own pace	3.5	3.7	0.2*
Low fees	3.3	3.6	0.4*
Opportunities to learn about the cyber security industry and typical roles	3.7	3.6	-0.1
Opportunities to engage with industry/potential employers	3.7	3.5	-0.2*
Government backing	3.0	3.3	0.2*
Access to Teaching Assistants/Subject Matter Experts to aid learning	3.4	3.1	-0.3*
Opportunities to engage with other candidates	3.0	3.0	0.0
Soft skills content (e.g., communication, teamwork)	3.2	2.9	-0.3*
Face to face	2.3	2.2	-0.1

Source: Ecorys analysis of SANS data
Indicators in the table are scores of 1-4, with 1=Not at all important*, 2=Slightly important, 3=Quite important, and 4=Very important.*
The symbol '' marks if a difference between before and after means is statistically significant at the 5% level.*

Additional outcomes

As well as expected outcomes relating to knowledge, skills, awareness and interest, students identified several additional outcomes when asked what they thought they had gained from participating in the programme.

This included improved knowledge of personal security, which students noted they could share with friends, family and colleagues. A major theme from students in technology or computing based existing roles was that they had been able to apply their newly acquired skills and knowledge to their current job. Some students reported that this may lead to promotions in their current role, or opportunities to set up cyber security functions or expand the services offered to clients.

> "[The programme has] given me more insight into the attack surface, what to look out for, how to prevent stuff, what to do in terms of monitoring and logging. I'll be going back and looking at my existing systems, ways to harden them. It's been useful if only for that."
> *Student*

Some students said that they were pursuing further cyber security related qualifications or training, in order to further specialise in a particular field. Some were pursuing further training in order to apply for particular job roles within cyber security, for example some students with existing careers were reluctant to move into a lower paid entry level position, so were looking to further upskill in order to secure higher paid roles. For others, this related to their current job role and they had secured funding from their employer to attend further training.

> "I have managed to qualify for a further SANS course, which work have now agreed to pay for because they are starting to see the value in me doing it. For example, I deal a lot with the National Cyber Security Centre and I've sat in meetings with them before where I've literally had no clue what they were talking about. I had a conversation with them this week about a proposal that they'd sent to us and I knew what it all meant and I understood it all. I can actually do my job better because of this understanding that I've now got."
> *Student*

A minor theme was that participating in the programme helped some students to develop or improve their study skills, which gave them confidence to pursue further training in the future.

> "It's been a while since I did any studying intensively so the confidence that I was able to take that on and pass the exams and get it all done within the timescale is a is a really big plus as well."
> *Student*

A further minor theme was that students developed a network of peers and industry professionals, who they would be able to keep in touch with after the programme ended. This was perceived as long-term support that would

potentially help them throughout their career in cyber security, beyond the initial period of securing an entry level role.

Outcomes for employers

Interviews with employers suggested that involvement in the programme was beneficial for them as individuals and their wider organisation. Although none of the employers that were interviewed had recruited a programme participant at the time of the interview, a major theme was that the programme was “worthwhile on a personal and organisation level’ and employers viewed any recruitment of programme participants as a bonus.

Personal outcomes identified by employers included a sense of satisfaction from supporting people to get into the cyber industry and the opportunity to develop mentoring skills. Organisational outcomes tended to focus on the opportunity to increase exposure as a cyber security employer, in particular the ability to reach a more diverse group of candidates and the potential for programme participants to apply for roles at their organisation. Wider outcomes were supporting a diverse range of individuals into the industry in order to bolster the cyber security workforce and nurturing a relationship with SANS which it was hoped could lead to collaboration on other programmes.

Conclusions

The Upskill in Cyber programme has exceeded all KPIs, except the 50% target for female applicants. This was recognised as an ambitious target substantially above the sector average of 22%, and feedback suggested that the comprehensive marketing and recruitment campaign to attract diverse applicants, targeting key demographics and leveraging existing non-profit partners was effective in attracting female candidates. It is recommended that future phases or programmes allocate additional budget to such marketing campaigns to ensure more female candidates apply.

Motivations for applying to the programme focused on the opportunity to develop cyber security skills in order to secure a job in the sector. Specific factors included the fact that the programme was fully funded, government backed and offered a flexible delivery model. Employers highlighted the opportunity to give back to the sector by supporting diversity and upskilling, and to meet potential candidates for entry level roles.

In terms of functionality of the platforms and online materials, students overall found them easy to use, and the majority of students were satisfied with the exam environment remotely and in test centres. Interviews suggested that students preferred the delivery style and platform used for the SEC275 course, and a strong theme was that more time was required for the SEC401 course and students would like to see this reflected in the delivery timescales.

Survey data and feedback from interviews suggested a significant increase in cyber security knowledge, skills, awareness, and career interest after participating in the programme. Students also reported higher levels of knowledge and skills in computing in general, but not higher interest in training and careers in computing. Students' perceptions of outcomes largely focused on technical skills, but interviews also highlighted increased motivation, confidence, and awareness.

In terms of cyber security careers, students reported higher levels of knowledge and confidence around pursuing a career in cyber (e.g., understanding the pathways, knowledge of skills and qualifications needed), and reported that the programme was very helpful to position them to pursue this. A major theme from interviews was that the programme accelerated students' journey into a career in cyber security, and that they would not have developed such a range of skills without the Upskill in Cyber programme. At the time of reporting (14th November 2022), 39 students had secured jobs in the cyber security sector which they mostly attributed to the programme, while others had secured interviews (58), were applying for jobs, or were finishing their training (40). Interviews highlighted the value of additional career focused elements of the programme, such as the careers fair, mentoring and soft skills sessions in raising awareness of the diversity of cyber security roles and possible routes into the sector.

Survey data also highlighted that students found the training courses and exams challenging in terms of their difficulty, especially the SEC401 course and GSEC exam. However, they reported that they enjoyed the programme, and almost all students said they would recommend this to someone else. At the time of reporting, most students (149) had passed both exams and 40 had passed their GFACT exam but were awaiting their GSEC exam.

Recommendations

Based on the evidence and feedback provided by students, employers, delivery provider, and policy stakeholders, the following recommendations are made in terms of **applications and programme delivery**:

- Improve efficiencies in the selection process and data collection at the application stage by applying mutually exclusive categories of accepted, “maybe” and declined applicants to reduce the time it takes to select accepted applicants.
- Additional support for employers looking to introduce entry level roles to their organisation, for example guidance on job descriptions and job requirements, and how to upskill those with lower levels of experience.
- Adjusting or extending delivery timelines is recommended to allow more time for the GSEC course, and to meet the needs of students with work and family commitments.
- Additional marketing and promotion aimed at targeting female applicants, building on the successful approaches identified by the delivery provider (SANS), for example leveraging non-profit partners. A longer marketing campaign duration (SANS recommend a minimum of six weeks) would allow for further optimisation and testing.
- More tailored support and guidance for career changers, as interviews suggest these students can face additional barriers to entering entry level positions, for example a reluctance to undertake roles with a lower salary than their current role and uncertainties about the relevance of transferable skills.
- Update the delivery platform used to deliver the SEC401 to be more appealing to students.[26]

The following recommendations are made about how to enhance future **data collection**:

- It is proposed that one post-exam only survey is sufficient to gather the data needed to understand students’ knowledge, awareness and perceptions after the completion of the programme. As there were no significant differences between post-training and post-exam responses, it is not necessary to collect responses at two separate time points. The timing of the final exam was also very soon after the training took place, which explains why students responded similarly to both surveys (for example there is very low risk of respondents not recalling what happened a few days/weeks after completing the course). It is also worth noting

[26] During the delivery of Upskill in Cyber, SANS rolled out an updated version of the OnDemand platform. The new player was designed in response to student feedback and includes a modernised interface with improved accessibility, easy to access help and support, an improved layout for the course outline, course notes, and search, as well as prominent course progress information allowing users to monitor progression. At the time of student interviews, this updated version had not yet been rolled out.

that future data collection could extend further than a few weeks to capture all students completing their exams. As noted above, the cut-off of the data collection period meant that some students had not had the chance to receive and complete the survey as they were still completing their training and exams.

- The introduction of a follow-up survey six to twelve months after students complete the course could provide further insight into the long-term impacts of the programme. As mentioned above, surveys and interviews showed that students were already securing jobs and engaging in interviews and applications in the cyber security sector. It can be expected that the status of applications and employment in cyber jobs would be different 6-12 months after the programme, as longer term outcomes and impact would have had time to materialise.

Annex One: Methodology

This annex provides a brief guide to the main elements of data collection for the Cyber Explorers evaluation to date and which form the basis of this report.

Surveys

Overall, there were 4 separate surveys, implemented by SANS:

1. Application (and baseline) survey
2. Post-training survey
3. Post-exam survey
4. Non-participant survey (aimed at applicants who did not get accepted into the programme)

The application and baseline survey contained 1,876 respondents. Applicants were asked to provide key demographic characteristics such as age, gender and ethnicity, answer questions around the functionality and accessibility of the training, as well as certain questions on their levels of knowledge, skills, awareness, and interest on cyber security and computing. The data also contains the applicants' CTE scores (overall and aptitude) which were the key indicators used to determine which applicants are offered a place in the programme, as well as an indicator of who was accepted in the programme. Based on the latter, we were also able to use two sub-samples for analysis: 217 accepted participants and 1,659 declined applicants.

The post-training and post-exam surveys collected 45 and 82 responses, achieving 40% and 77% response rates (45 out of 113 and 82 out of 107 invites). The total number of students responding to both surveys was 103, as 21 students responded only to the post-training survey, 58 responded only to the post-exam, and 24 responded to both. The post surveys had an overall response rate of 72%, based on the total number of accepted students who received a post-training and/or a post-exam survey (103 out of 143 students completing training and exams). We were able to match all 103 respondents against the baseline survey, achieving a pre-post sample size of 103 for our analysis. It is worth noting that the post surveys were not sent to all 217 accepted students, as 26 withdrew from the programme or paused their training, while 40 students were yet to sit their final GSEC exam.

Post-training and post-exam responses were compared to identify potential differences between them. The comparison showed no significant differences between key outcomes (apart from only one indicator), suggesting that respondents were answering both surveys similarly. This is very positive as it provides further validation of survey results, especially considering limitations of self-reported measures (as mentioned in the Data limitations section). This also suggests that one post-exam survey should be sufficient to

capture all the necessary information, minimising resources spent on survey design and dissemination, as well as potential survey burden on students. The latter is very important as it could be key in getting even higher response rates, thus collecting more data in future surveys. The following table outlines the comparisons made across all indicators for the two surveys:

Outcome	Scale	Post-training (n=38)		Post-exam (n=85)		Difference
		Mean	SD	Mean	SD	
Cyber security knowledge and skills	0-3	2.7	0.5	2.7	0.6	0.1
Cyber security awareness	0-3	2.7	0.5	2.7	0.5	0.0
Cyber security career awareness	0-3	2.1	0.6	2.2	0.7	0.1
Computing knowledge and skills	0-3	2.7	0.5	2.7	0.5	0.0
Cyber security career interest	0-10	8.8	1.7	9.3	1.3	0.5*
Cyber security training interest	0-10	8.9	1.7	9.2	1.6	0.2
Computing career interest	0-10	8.3	2.1	8.8	1.6	0.5
Computing training interest	0-10	8.8	2.0	8.9	1.9	0.1
Equipped for a cyber career	0-10	7.9	1.8	8.2	1.4	0.4
Knowledge of steps needed to pursue a career in cyber security	1-5	4.2	0.7	4.2	0.8	0.0
Knowledge of skills needed to pursue a career in cyber security	1-5	4.2	0.7	4.2	0.6	0.0
Knowledge of qualifications needed to pursue a career in cyber security	1-5	3.9	0.9	4.0	0.8	0.1
Knowledge of where to get information about pursuing a career in cyber security	1-5	4.0	0.7	4.1	0.8	0.1
Lack of sufficient knowledge about cyber security in general to know if it is a career option	1-5	2.1	1.0	1.9	0.9	-0.3
Confidence of being ready to work in a cyber security role	1-5	3.7	0.9	4.0	0.8	0.2
Understanding of career pathways available in cybersecurity	1-5	4.0	0.7	4.0	0.8	0.0

Statistically significant differences are marked with an asterisk '' and are estimated at the 5% level.*

Source: Ecorys analysis of SANS data

It is worth noting that the samples used for this comparison were 38 responses from the post-training survey and 85 from the post-exam. These are slightly different to the original samples in the raw data (45 and 82 respectively), as some respondents answered the post-training survey after they took the exam. These responses were treated as though they were post-exam responses, to improve the accuracy of these comparisons.

Lastly, the non-participant survey collected 93 responses. This means the survey achieved a response rate of almost 6%, based on the total number of declined applicants (93 out of 1,659). This was much lower than the participant post surveys, although this was expected as declined applicants might feel less inclined to engage. It is worth noting that there was some negative feedback from declined applicants as they did not understand why they were contacted. In addition, we acknowledge that declined applicants who chose to respond to this survey might be more inclined to answer negatively about the programme, which should be an important consideration for future data collection and analysis on this cohort.

Survey data analysis

Data collected by the above surveys was provided by SANS and all analysis of survey data was done by Ecorys and Perspective Economics. We undertook the following types of analysis using all survey data available:

1. Baseline analysis: understanding the profile of applicants (n=1,876) and comparing the key characteristics of accepted (n=217) vs not accepted applicants (n=1,659).
2. Pre-post analysis: comparing the key outcomes (knowledge, skills, awareness, interest) of accepted applicants before and after they took part in the programme (n=103).
3. Analysis on secondary questions: a set of secondary questions were asked across all surveys, for example on levels of enjoyment, perceived levels of difficulty, functionality of the online platforms, etc. Some of the questions were only asked in post, others both in pre and post, and some only in post-training or post-exam. Sample sizes are dependent on each specific question and data source.
4. Qualitative analysis of open text responses: in some cases, respondents were asked to elaborate on their answers with text, which was analysed and interpreted alongside other qualitative and quantitative evidence
5. Feasibility assessment: taking into consideration response rates across all surveys, acceptance rates and acceptance criteria, informed by all analysis in

this report, and using baseline data to simulate potential designs for impact evaluation

The pre-post analysis is at the centre of estimating potential outcomes and impact caused by participating in the Upskill in Cyber programme. The analysis entailed estimating the differences between mean scores of accepted students before and after taking part and testing those differences for statistical significance. This included running a paired t-test to identify statistical significance at the 5% level. As noted above (see data limitations section), the pre-post analysis is not meant to replace an impact assessment of the programme, but to provide with initial indications of impact. Further impact analysis will need to be done to identify the true impact of the programme, as noted in the feasibility assessment (see Annex six).

All quantitative analysis and data visualisation in this report was made using R Studio, Microsoft Excel, and Tableau.

Student interviews

This report draws on feedback from 37 interviews conducted in August, September and October. Interviews were conducted remotely by telephone and MS Teams and explored motivations for applying to the programme, views on content and delivery models, perceptions of outcomes and next steps relating to cyber security careers.

Policy interviews

Ten policy interviews were conducted, covering both strands of the evaluation (Cyber Explorers and Upskill in Cyber). Of these ten interviews, three focused on the Upskill in Cyber programme, while the remaining seven focused on Cyber Explorers. These were conducted remotely by telephone or MS Teams and explored how the programme links to wider policy, how the evaluation can help inform future programmes, and early lessons learnt.

Employer interviews

Five interviews were conducted with employers who supported the programme through for example, mentorship, attendance at careers fairs and input to soft skills sessions. These were conducted remotely by telephone or MS Teams and explored reasons for involvement in the programme, views on outcomes for industry and students, and possible future involvement in such programmes.

Annex Two: Research questions

This annex outlines the research questions identified in the invitation to tender.

Cyber Security Adult Training Pilot		
Process	Marketing	How effective was the programme marketing in ensuring the programme attracted sufficient applicants?
		How successfully did the campaign target, and attract, its intended audiences (with particular regards to characteristics of interest e.g., gender, ethnic minority groups, location, socioeconomic status)?
		What communications channel or mix of channels were most effective in reaching the target audience?
		What motivations and drivers can future campaigns plug into to better engage with the target audience? What has been the wider learning for future adult skills programme marketing campaigns?
	Recruitment, Selection & Retention	How effective was the application process in ensuring sufficient numbers of suitable applicants?
		What were the barriers / enablers to successful student applications?
		How effective was the selection process i.e., did it successfully identify candidates with an aptitude and interest in pursuing a career related to cybersecurity?
		What were the barriers / enablers to the selection process?
		To what extent did the programme successfully retain participants?

		What were the barriers / enablers to the retention of programme participants?
		Did the recruitment, selection and retention process work to effectively support those with characteristics of interest?
	Programme Delivery	Was the programme delivered as described in the Theory of Change? Were the assumptions laid out in the ToC met?
		How did the rollout of the programme differ across pilot areas?
		What were the reasons for any differences?
		To what extent has the programme been able to adapt to any varying needs or circumstances within the pilot areas?
		Have the programme delivery partners met our expectations (goals, KPIs etc)?
		To what extent was the digital platform an effective way of delivering the intervention?
		What were the barriers and enablers to the delivery of the programme and its objectives?
		What has this programme taught us about how similar future initiatives can be improved?
		Did the programme make suitable accommodations for professional or personal commitments of applicants?
Impact	Outcomes &	To what extent have applicants gone on to i) be interviewed and ii) secure employment in the cyber industry; (particularly for participants with targeted characteristics)?

	Impacts	Did the programme deliver any unintended benefits, or cause any unanticipated adverse consequences?
		What has been the feedback on content and training from stakeholders (e.g., cyber industry organisations, employers)?
		How successful was the programme in equipping participants to successfully complete Cyber Essentials assessments?
Value for Money	To what extent has the programme delivered value for money?	
	Which elements of the programme provided the most value?	
	What learning could be taken into future programmes to improve returns on investment in the future?	

Annex Three: Selection process

The current selection process is based first on a set of key eligibility criteria with the CyberTalent Enhanced (CTE) aptitude assessment score acting as the key determining factor. The CTE aptitude and overall test scores are taken into consideration when selecting candidates (scores with minimum 0% and maximum 100%):

- Accept: Candidates scoring >64 in Information Security Aptitude and >64 in Overall.
- Decline: Candidates scoring <56 in Information Security Aptitude and <50 in Overall.
- Maybe:
    - Candidates scoring >70 in Information Security Aptitude and <50 in Overall.
    - Candidates scoring 56-64 in Information Security Aptitude and 50-64 in Overall.

Candidates under “accept” are first accepted into the programme and if places remain, candidates from the “maybe” pool are considered based on other factors in their application such as their motivations, existing experience and transferrable skills. However, these categories are not mutually exclusive as there are candidates who do not fit in any of them. For example, a candidate with a CTE aptitude score of 76 and an overall score of 62 does not fit in any of the above categories, although their scores are relatively high and they are likely to be considered. These applicants are then treated as case-by-case, to identify whether they should be accepted or not. Defining clear cut-offs with mutually exclusive categories would reduce the resources needed for this process, and improve efficiency especially in the case the programme is scaled up to larger numbers.

Clear cut-offs based on test scores could also prove useful in designing a regression discontinuity design (RDD) for an impact assessment of the programme (see Feasibility Assessment in Annex six).

Annex Four: Programme schedule

Schedule

	Study/Exams	Extra-curricular Activities
Week 1 4th - 8th July	**Course 1** SEC275: Foundations - Computers, Technology, & Security	Welcome & Introduction
		Soft Skills / Employer Session
Week 2 11th - 15th July	**Course 1** SEC275: Foundations - Computers, Technology, & Security	Soft Skills / Employer Session
Week 3 18th - 22nd July	**Course 1** SEC275: Foundations - Computers, Technology, & Security	Soft Skills / Employer Session
Week 4 25th - 29th July	**Course 1** SEC275: Foundations - Computers, Technology, & Security	Soft Skills / Employer Session
Week 5 1st - 5th August	GFACT Exam Window	

	Study/Exams	Extra-curricular Activities
Week 6 8th - 12th August	**Course 2** SEC401: Security Essentials: Network, Endpoint, and Cloud	Soft Skills / Employer Session
Week 7 15th - 19th August	**Course 2** SEC401: Security Essentials: Network, Endpoint, and Cloud	Soft Skills / Employer Session
	Course 2 SEC401: Security Essentials: Network, Endpoint, and Cloud	
Week 8 22nd - 26th August	**Course 2** SEC401: Security Essentials: Network, Endpoint, and Cloud	Careers Fair
Week 9 29th August - 2nd September	**Course 2** SEC401: Security Essentials: Network, Endpoint, and Cloud	
Week 10 5th - 9th September	GSEC Exam Window	Online Capture The Flag Competition (CTF)
		Graduation

- Course Study: Self-paced study
- Course Study: Instructor Led (Fixed Hours)
- GIAC Exam Window
- Self Study/Down-time
- Extracurricular Activities: Soft Skills & Employability
- Additional Hands On Training

www.upskillcyber.co.uk

SANS | HM Government | SKILLS FOR LIFE

Annex Five: Glossary

Term	Definition
Student	An accepted applicant who participated in the programme
CyberTalent Enhanced Assessment (CTE)	CTE Assessments are web-based and feature 50 questions (25 skill-based and 25 aptitude-based questions). Each user has a unique link with 120 minutes to complete the Assessment. Online reports summarise each user's results in detail and are only accessible to a designated report manager. Users do not see their own results at the completion of the Assessment.
SEC275: Foundations-Computers, Technology & Security	Course 1 of the programme. A course overview is available at: https://www.sans.org/cyber-security-courses/foundations/
SEC401: Security essentials: Network, Endpoint, and Cloud	Course 2 of the programme. A course overview is available at: https://www.sans.org/cyber-security-courses/security-essentials-network-endpoint-cloud/
Delivery provider	The provider, SANS, contracted by government to deliver the Upskill in Cyber programme.
Slack	Slack is a messaging app for business that connects people to the information that they need. Available at: https://slack.com/intl/en-gb/help/articles/115004071768-What-is-Slack-
GFACT	The GIAC Foundational Cybersecurity Technologies (GFACT) certification validates a practitioner's knowledge of essential foundational cybersecurity concepts. The GFACT exam is sat at the end of the SEC275 course. Full details available at: https://www.giac.org/certifications/foundational-cybersecurity-technologies-gfact/
GSEC	The GIAC Security Essentials (GSEC) certification validates a practitioner's knowledge of information security beyond simple terminology and concepts. The GSEC exam is sat at the end of the SEC401 course. Full details available at: https://www.giac.org/certifications/security-essentials-gsec/

Annex Six: Feasibility assessment

Introduction

In this annex we outline our feasibility assessment for a counterfactual impact evaluation (CIE) of the Upskill in Cyber programme. A CIE will in turn assess the impact of the programme on students' knowledge, skills, awareness, and interest around cyber security and pursuing careers in the sector. During phase 1 of the programme, we assessed early indications of impact by comparing key outcomes on cyber security before and after students participated in the programme. As the programme continues into a second phase, we explore the feasibility of assessing the impact of the programme as a whole across both phases.

Overall, our assessment has found that a CIE would be feasible at the end of phase 2, focusing on two promising designs: a Regression Discontinuity Design (RDD) as the primary option, and an Inverse Probability Weighting (IPW) approach as the secondary option.

Feasibility assessment approach

Our feasibility assessment approach is based on key international and UK-based guidance such as the Magenta Book[27], starting from assessing the feasibility and appropriateness of a randomised experiment or Randomised Control Trial (RCT), then potential Quasi-Experimental Designs (QED), and lastly theory-based approaches.

Our assessment approach followed these broad inter-related considerations:

- **Programme design:** We investigate key elements of the programme which affect the feasibility of a CIE, starting from the application and selection process. The process which determines how the 'treatment' is allocated (i.e., how students are selected to participate), also determines which type of CIE (if any) is feasible or appropriate. A key aspect of this is to determine whether a 'comparator group' (i.e., those not receiving the benefits of the programme) is available or can be constructed, to be compared against the beneficiaries of the programme (the 'treatment group').
- **Outcomes and data:** We first determine which are the outcomes of interest and whether these are measurable. We assess data availability on key outcome indicators and any other data required for a CIE. This includes the feasibility of primary

27 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/879438/HMT_Magenta_Book.pdf

collection through surveys, and achievable sample sizes required for impact to be detected.

- **Programme and evaluation timing**: We assess whether impact is expected to materialise within the lifetime of the programme, as well as if the evaluation timelines allow for data collection and impact analysis to be conducted.
- **Methods:** Lastly, we assess whether one or multiple CIE methods are feasible and appropriate to assess the impact of the programme. We explore the feasibility of key methods such as difference-in-differences, matching and weighting techniques, instrumental variables and other methodologies widely recognised in the literature.

Treatment and comparator groups

A key consideration for any feasibility study is to assess whether treatment and comparator groups can be identified or constructed for comparison, as this is a key element in the design of CIEs. During phase 1 we have already identified these as below:

- **Treatment group:** all accepted students receiving training through the Upskill in Cyber programme
- **Comparator group:** declined applicants who did not get into the programme[28]

In a CIE, the two groups are compared against each other (most likely over time as well), and any differences found between them is the impact of the programme. One of the key considerations here is that the two groups should be as similar as possible to ensure that comparisons are robust. As both groups contain eligible applicants, they are considered to be broadly comparable, however during phase 1 we found some differences in their demographic characteristics (see Table 3). We aim to update those comparisons using the new data in phase 2, to identify if there are still differences, and to ensure we would successfully control for those. Specific QEDs considered below aim to control for such differences by filtering or weighting the data.

It is worth noting that treatment and comparator groups from phases 1 and 2 would most likely be combined to assess the impact of the programme across both phases. As noted below, this would also allow us to make use of larger samples capable of detecting impact with higher statistical power.

[28] It is likely that some of the declined applicants from phase 1 with high CTE scores will be considered to be accepted in phase 2, in which case they will be removed from the comparator group.

Outcomes & data

Outcomes of interest and indicators

The key outcomes and indicators of interest for a CIE would be the same used in the quantitative analysis of phase 1, covering knowledge, skills and awareness in cyber security, interest in cyber security and computing, and knowledge and confidence regarding cyber security careers. Separate indicators were used to measure these outcomes in the form of Likert-style survey questions (e.g., a scale of 1-5, with 1 being "strongly disagree" and 5 being "strongly agree". The outcomes and full list of indicators are shown below:

Table 1 Outcomes of interest and indicators

Outcome theme	Outcome indicator
Knowledge, skills, and awareness	• Cyber security knowledge and skills • Cyber security awareness • Cyber security career awareness • Computing knowledge and skills
Interest in cyber security and computing	• Cyber security career interest • Cyber security training interest • Computing career interest • Computing training interest
Knowledge and confidence on cyber security careers	• Knowledge of steps needed to pursue a career in cyber security • Knowledge of skills needed to pursue a career in cyber security • Knowledge of qualifications needed to pursue a career in cyber security • Knowledge of where to get information about pursuing a career in cyber security • Confidence of being ready to work in a cyber security role • Understanding of career pathways available in cybersecurity • Lack of sufficient knowledge about cyber security in general to know if it is a career option

As tested during the analysis of phase 1 data, the above indicators are overall good measures of outcomes and impacts of the Upskill in Cyber programme. However, they present with a few challenges and caveats, which will also have to be taken into consideration during any phase 2 analysis (see Data limitations section above for more detail).

Surveys

During phase 1, SANS distributed baseline and post surveys to both accepted students and non-participants, collecting data which was then used for our quantitative analysis. We suggest that this process should be repeated in phase 2, to allow us to use this data for a potential CIE. However, as noted in our recommendations, we suggest that the two post-training and post-exam surveys are combined into one, potentially boosting response rates and minimising survey fatigue among applicants/participants.

We will also consider ways of boosting responses in the non-participant survey as this will be crucial in determining the final sample size of the comparator group.

Methodology

In this section we explore the feasibility and appropriateness of key CIE methods. Our assessment suggests that **randomised experiment or RCT approaches are not feasible**, as the 'treatment' (participation in the Upskill in Cyber programme) is not randomly allocated. This is because eligible applicants are first selected through a screening process at the start of their application, and then students are accepted into the programme based on their performance on their CyberTalent Enhanced[29] (CTE) test scores. The non-random recruitment and selection process does not allow us to apply a randomised experiment approach to assess impact, while it also might introduce a 'selection bias' which needs to be controlled for. For example, if selected students are on average more knowledgeable in cyber security subjects compared to not selected students, this could lead to an overestimation of the impact of the programme.

We therefore focus on **quasi-experimental designs (QEDs)** as the most feasible and appropriate options for an impact evaluation, as these can control for this type of bias and provide robust estimates of impact. During our assessment, we explored the feasibility of several QEDs, as outlined in the table below.

Table 2 Feasibility of QED methods

Method	Feasibility

[29] https://www.sans.org/cybersecurity-assessments/enhanced/

[30] Instrumental Variables (IV) was also considered in this assessment, but it is outlined as a specific analysis under RDD, as opposed to a separate method (see 'fuzzy' RDD in below sections).

Difference-in-differences (DID)	**Feasible but not sufficient.** DID analysis could be implemented as it is likely to have data for both treatment and comparator groups (accepted and not accepted applicants), as well as over time (before and after participation in the programme). DID assumes that any differences between the two groups remain the same over time[31], meaning the groups should be as similar as possible. As shown in the phase 1 analysis, the two groups might be different in terms of their characteristics. While DID controls for differences in characteristics which are constant over time, it does not control for characteristics which might be affecting outcomes in different ways over time (e.g., a higher proportion of males in the treatment group affecting changes in the outcome after taking part in the programme). There is no way of testing this as we cannot know what would have happened to the same people if they did not take part in the programme (i.e., whether the 'counterfactual trend' is parallel to the treatment group trend). Matching or weighting techniques, either as standalone methods or paired with DID, can improve on DID comparisons and robustness of impact estimates. We would test the similarity of the two groups when we have phase 2 data.
Interrupted time series analysis (ITS)	**Not feasible/appropriate.** Although advantageous as it does not need a comparator group, this method requires data across multiple time points in order to build a counterfactual trend. ITS usually requires at least 8 time points before and 8 after the intervention (participation in the

[31] Known in the literature as the 'parallel trends assumption'.

	programme), which would not be possible in this case.
Regression Discontinuity Design (RDD)	**Feasible.** RDD is feasible in terms of requirement of an 'eligibility' score with a cut-off (in this case CTE scores), as well as data requirements which can be met with pre-post surveys across accepted and not accepted applicants. Certain caveats remain in terms of sample sizes, and whether those would be sufficient to compare smaller sub-samples just above and below the cut-off point.
Matching/Weighting methods	**Feasible.** Matching or weighting methods are feasible in terms of data requirements as they can be met through pre-post surveys across accepted and not accepted applicants. We suggest that Inverse Probability Weighting (IPW) is a better option compared to other methods, as it has the advantage of maintaining the whole treatment group sample. However, caveats remain around the sample size of the comparator group, as this might be reduced further due to weighting.

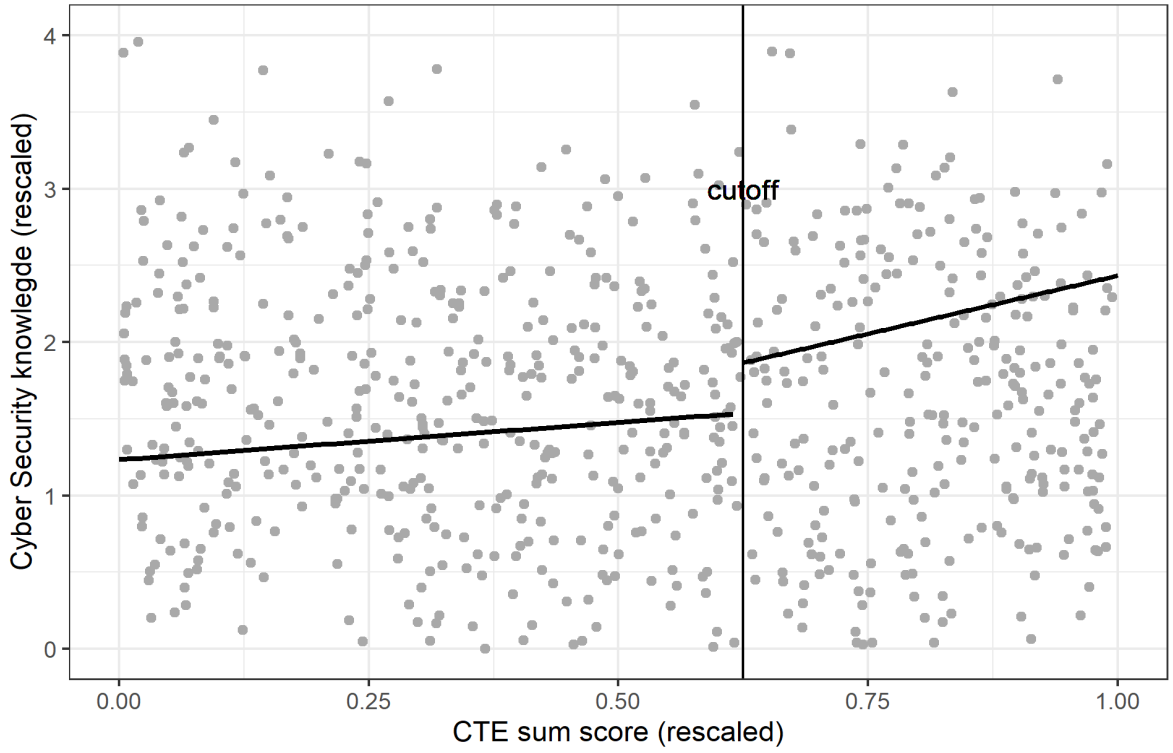
We have concluded that the most feasible and appropriate QEDs are Regression Discontinuity Design (RDD) and Inverse Probability Weighting (IPW) methods, which are outlined in detail in the following sections. Difference-in-differences (DID) is also feasible but might not be sufficient to fully estimate impact. This however can be tested further during the impact analysis, to provide with additional validity to the impact estimates (for example comparing DID and IPW results).

Regression Discontinuity Design (RDD)

In cases where a score or threshold value is used to determine who does and who does not receive an intervention, a regression discontinuity design can be used to estimate the impact of the intervention. The variable used to allocate treatment is termed the "running variable", and the threshold that determines treatment, the "cut-off". Those on one side of the cut-off are allocated a treatment, those on the other are not. To estimate impact using this method, the average outcome levels of the treated and untreated groups (either side

of the threshold) are calculated and compared. The change/jump ("discontinuity") in the outcome variable at the cut-off provides with the impact estimate (illustrated in Figure 1[32]). As noted above, a key consideration when conducting a CIE is that the treatment and comparison group should be as similar as possible to ensure comparisons are robust. In an RDD, those just below and just above the cut-off are usually compared, as they are assumed to be the most similar.

Simulation of RDD analysis using phase 1 baseline data



In this case, the CTE aptitude, the CTE overall score, or a combination of both, would be used as the running variable. In phase 1, SANS used the following acceptance process:

Table 3 CTE cut-offs in the selection process

Application outcome	Score ranges
Accepted	CTE overall > 64 & CTE aptitude > 64
Declined	CTE overall <50 & CTE aptitude <56
Maybe	CTE overall <50 & CTE aptitude >70 CTE overall 50-64 & CTE aptitude 56-64

[32] In this figure, variables are rescaled to illustrate a typical RDD visualisation. Cyber security knowledge was increased by an arbitrary 0.3 points for those above the cut-off, to simulate how this discontinuity in outcome levels would look like.

In order for regression discontinuity to be appropriate/internally valid, certain conditions must be met. The table below lists these conditions, and how they are met or are likely to be met for the Upskill in Cyber programme.

Table 4 RDD conditions and rationale

Condition	Met/rationale
Running variable cannot be caused/influenced by treatment (i.e., it is measured prior to the start of treatment or is one that can't be influenced by treatment)	**Met.** The CTE aptitude/overall scores of applicants would be used as the running variable; these are measured prior to treatment
Cut-off point is determined independently of the running variable (i.e., the threshold is not decided based on knowledge of student scores)	**Met.** The threshold for applicants was set by SANS without knowledge of the individuals who would be above/below the threshold
Nothing other than treatment is causing a discontinuity in the outcome of interest at the cut off (e.g., if the scoring threshold meant individuals receive multiple treatments, we would only be able to study impact of combined effects of treatments)	**Met.** It is reasonable to assume that the only treatment that was allocated based on the CTE aptitude/overall scores was the Upskill in Cyber programme
In the absence of the treatment of interest, there is no discontinuity in the outcome at the cut-off (meaning any change at the cut off can be attributed to the treatment)	**Met.** Whilst there is no exact test for this, we have tested by plotting the pre-treatment data for the 9 outcome variables against the running variable and found no visible discontinuity at the cut-off in any case. This indicates that any change detected in the post-treatment data could be attributed to the programme.

Data requirements

In order to run an RDD we would use application data and post-treatment outcomes data as outlined in the table below. Depending on the approach taken, pre-treatment outcome data may be used to inform the model.

Table 5 RDD data requirements

Element	Data requirement

Treatment group	Post-treatment outcomes of individuals who were accepted and took part in the programme.
Comparator group	'Post-treatment' (collected at a similar timepoint to the post-treatment data) outcomes data of individuals who were eligible but not accepted.
Running variable	The CTE aptitude or overall score for the treatment and comparator groups. The application data should include a variable on whether individuals were accepted or declined and a reason for decline where required (to determine eligibility). This will be used to calculate the probability of treatment.
Controls or instruments	Depending on the approach taken (discussed below), some variables may be included as controls. For instance, if using a 'fuzzy' design and/or a large bandwidth, the use of control/instrumental variables can be required to account for bias and reduce standard errors.
Informing approach	The pre-treatment outcome data can be used to understand the relationship between the outcome and running variable and inform the selection of the most appropriate regression model.

Approach considerations

Below we discuss factors that will be considered to determine the most appropriate RDD approach based on the complete dataset following phase 2. These include: selection of the running variable; sharp or fuzzy design; model selection and; sample size. These factors are interconnected and will be considered alongside one another.

1. Selection of the running variable

As noted above, there is not one score that determines whether an applicant is accepted or declined. The acceptance decision is based on both the CTE aptitude and CTE overall

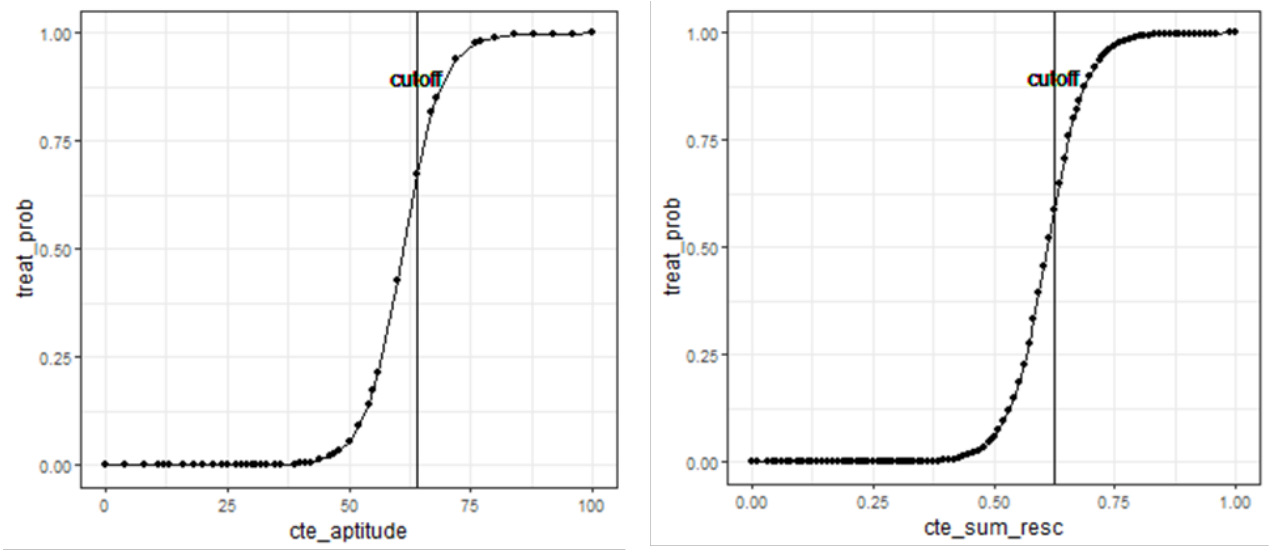
score and, for those in the “maybe” category, other qualitative factors such as previous work or training experience are taken into consideration. Each of the following would be tested as to how well they predict the number of accepted students compared to the actual number of accepted students:

- Sum the CTE scores with the threshold set as the sum of CTE thresholds. The index would be rescaled to 0-1 to make interpretation of regression coefficients easier.
- Use the CTE aptitude as a proxy for selection as this is the priority that SANS uses in application decisions.
- Use the CTE overall and aptitude as independent running variables.

2. ‘Sharp’ or ‘fuzzy’ design

The impact estimate in RDD is based on the effect of treatment around the cut-off. In many real-world scenarios the cut-off is not exact (i.e., there is a “maybe” category in which factors other than the running variable are used to allocate treatment). In these cases, a “fuzzy” design should be used. In a “sharp” design, the probability of treatment (i.e., the probability of being accepted into the programme) for an individual jumps from 0 to 1 at the cut-off. In a fuzzy design the probability of treatment increases gradually around cut-off.

Using data from phase 1, we calculated the probability of treatment using the CTE aptitude score and the sum of CTE overall and aptitude scores as running variables (left and right respectively in the figure below).



Probability of selection into the programme based on CTE scores

Given that there is not a single score that determines acceptance, it is likely that we will use a fuzzy approach. SANS has indicated that they will use a more standardised acceptance process in phase 2, however it is likely that this will still include a "maybe" category in which case a fuzzy approach would be most appropriate.

Additional considerations include:

- If the selection process in phase 2 would allow for a sharp design, we would consider the trade-off between combing phase 1 and 2 datasets and gaining greater statistical power, and using only phase 2 data and gaining greater precision from using a sharp design[33].
- In phase 1, some applicants completed applications after all places on Upskill in Cyber had been allocated. We will consider how to address this group in analysis in terms of their probability of treatment (used in models in a fuzzy design) and as some of these applicants may be considered for phase 2 meaning they would have to be removed from the phase 1 sample.

3. Model selection

There are 2 statistical approaches for estimating the impact; parametric and non-parametric. The selection of the approach (and the precise model within each approach) will be determined by factors such as sample size and the nature of the relationship between the running variable (CTE aptitude/overall score) and outcome variable (e.g., knowledge in cyber security). In practice, we would test a variety of models and use diagnostic tests to determine which gives the most precise/accurate estimation of impact based on the phase 2/combined phase 1 and 2 data. Some considerations are:

- In a parametric approach, all the outcome data is included (not just that around the cut-off) which increases statistical power within a given sample size. However, it is more vulnerable to bias introduced by including all applicants and the need to fit an accurate regression model/line.
- In a non-parametric approach, only the data near the cut-off would be used (within a defined "bandwidth", see below) and a linear model fitted. This is less vulnerable to the biases outlined above but it reduces the sample size and hence statistical power, and requires selecting the optimum bandwidth.

4. Sample size and statistical power

We ran calculations to estimate what sample size we would need to have adequate statistical power, based on data from phase 1. The two samples we will be considering are the:

[33] https://www.mdrc.org/sites/default/files/regression_discontinuity_full.pdf (see page 67 for discussion on fuzzy vs sharp precision).

- Treatment group sample: **successful applicants** who have **responded to the post survey**
- Comparator group sample: **unsuccessful applicants** who have **responded to the 'post' survey**

The treatment group sample size is determined by both the number of places offered and the response rate of those taking part in the programme. The comparator group sample size is determined by both the number of overall applicants and the response rate of unsuccessful applicants to the 'post' survey. The numbers for phase 1 are shown in the table below (treatment group would be n = 103 and comparator group would be n = 93)

Table 6 Phase 1 samples

Measure	Successful applicants	Unsuccessful applicants
Number of individuals	217	1,659
Number of post survey responses	103	93
Rate	47%	6%

A recommendation for phase 2 would be to increase the response rate amongst both groups, for example through making the post-survey for course participants mandatory, or through incentivising responses. As noted above, we will consider combining data from phase 1 and phase 2, taking into consideration any changes to the application and/or course content and their implications on the analysis approach and interpretation of the findings.

Under a non-parametric approach, we would restrict the data included in the model to those around the cut-off in order to reduce potential bias on the impact estimate. The "bandwidth" is the range of the running score variable used in the model. For instance, if we set the bandwidth to 10, we would only include the outcome data for those with a CTE aptitude score of 54 to 74 (around the cut-off of 64) in our model. Having a smaller bandwidth means it is more likely to successfully reduce bias caused by variation between individuals further away from the cut-off. This is a trade-off against reductions in sample size and statistical power.

We ran power calculations to estimate the comparator group sample size[34] that would be required to detect a small or medium effect size, under a number of different approach scenarios. The scenarios tested include: using a parametric vs non-parametric approach (i.e., using all available data vs a restricted sub-sample of data); using phase 2 only data vs combining phase 1 and 2 data; and a number of different bandwidths (for non-parametric approach). Table 7 presents the results of 4 of these scenarios.

[34] Number of individuals in the comparator group sample (defined above).

For each scenario below, the **estimated treatment group size** and **estimated comparator group size** are based on Phase 1 data and/or predicated Phase 2 data[35]. The **required comparator group size,** the output of the power calculation, states the number of individuals that would be needed in order to have the power to detect the respective **minimum detectable effect size** (column 3). The last column states the required **response rate** amongst unsuccessful applicants that would be needed to achieve the required comparator group size, and our assessment on the **feasibility** of this given the response rates achieved in Phase 1 (6%, Table 6). All calculations use the standard parameters of statistical power of 80% and statistical significance level of 5%[36].

Table 7 Sample size estimations for different scenarios

Scenario	Estimated treatment group size	Estimated comparator group size	Minimum detectable effect size	Required comparator sample size	Required response rate and feasibility
Non-parametric, bandwidth of 12, phase 2 data only	45	14	*0.3*	*NA*	**Impossible**
			0.5	108	44% **Unlikely**
Non-parametric, bandwidth of 12, combined phase 1 and 2 data	94	21	*0.3*	1232	330% **Impossible**
			0.5	48	13% **Possible**
Parametric, phase 2 data only	95	95	*0.3*	1085	64% **Unlikely**
			0.5	48	3% **Likely**
Parametric, combined	198	145	*0.3*	157	6% **Likely**

[35] Estimated numbers of places offered in Phase 2 n=200, and estimated numbers of individuals at each score value (for scenarios with bandwidth). For example, in Scenario 1, based on phase 1 numbers, we estimate for phase 2 a total of 1700 unsuccessful applicants, a response rate of 6% and an estimated proportion of 14% of applicants scoring between 52-76 (bandwidth of 12). This means that the estimated comparator group size would be 14 people (1700x0.06x0.14=14).

[36] These are standard parameters used in the literature, which can be however relaxed if needed.

[37] The effect size here refers to the standard Cohen's d effect size, where 0.2 is a 'small' effect, 0.5 is a 'medium' effect, and 0.8 is a 'large' effect.

[38] amongst unsuccessful applicants

phase 1 and 2 data			*0.5*	38	1% **Likely**

Based on these calculations we conclude:

- There are a number of feasible options including both non-parametric and parametric approaches (Table 7). It is likely that we will need to combine the phase 1 and phase 2 datasets in order to achieve the required comparator sample size. This is especially likely to be required to detect a minimum effect size of 0.3. To use a non-parametric approach and detect a minimum effect size of 0.3, we would have to use a bandwidth of 36 or above.
- Achieving a greater response rate in the comparator group (unsuccessful applicants) will enable greater opportunity to select the most appropriate approach, and/or decrease the minimum detectable effect size. Whilst increasing the response rate amongst students would be positive, there is less scope for large increases, and thus the unsuccessful applicant group should be a priority.

Inverse Probability Weighting (IPW) method

As mentioned above, accepted students might be different in some of their characteristics compared to not accepted students, which might in turn affect outcomes and lead to biased impact estimates. Matching or weighting methods can account for those differences by improving the comparisons between the two groups. The Inverse Probability Weighting (IPW) method can achieve this by weighting the data, i.e., assigning higher or lower "importance" to the outcomes of specific individuals based on their characteristics. The weighted outcomes of the two groups are then compared against each other, and any detected differences between them show the impact of the programme.

The weights are estimated using a logistic regression model predicting the probability of treatment (i.e., the probability of being selected into the programme) based on key confounders. A weight of 1[39] (100%) is then assigned to the treatment group (the accepted students) and varying weights (more or less than 1) to the comparator group (the non-accepted applicants). A generalised linear model (GLM)[40] is then applied to produce impact estimates using these weights.

Data requirements

[39] The probability of an individual being selected based on their characteristics is known as a propensity score (PS). The IPW method assigns the inverse of that (1/PS) to each observation. As accepted students have 100% probability of being selected into the programme, they are assigned a weight of 1/1=1.
[40] A generalisation of ordinary regression analysis, commonly used in weighted models.

IPW would require the same data collected in phase 1 and required for the RDD, namely the baseline data for all applicants as well as the post survey data for both accepted and not accepted applicants. As above, the treatment group will be determined by the accepted students, and the comparator group by the unsuccessful applicants. Final samples will be dependent on the number of responses in the post surveys which are successfully matched to the baseline/application data.

The key variables used for the weighting would be the following demographic characteristics, also used in comparisons drawn during phase 1:

- Age
- Gender
- Ethnicity
- Area (based on KPI: in or outside of London and the Southeast)
- Education (post GCSE qualifications)
- Employment status

As the IPW analysis would be done at the post-level (after participating in the programme), we would also include the baseline outcomes in this weighting alongside all the above characteristics. This means that for each outcome indicator, we would run a separate model using all the above characteristics plus the levels of that outcome at the baseline. This is meant to control for any differences in the initial outcome levels of the treatment and comparator group. For example, if accepted students already had a higher cyber security knowledge compared to the declined applicants, their direct comparison at the post-level would likely overestimate the true impact of the programme[41].

Sample size considerations

Data from phase 1 and phase 2 are likely to be combined to achieve a bigger sample, as with the RD design. Assuming a combined sample of 200 accepted students[42], we would need at least 156 declined applicants in the comparator group to detect a relatively small (0.3) effect size (with a statistical power of 80% and statistical significance level of 5%). As the non-participant survey collected 93 responses during phase 1, and assuming a similar number of responses could be collected in phase 2 (i.e., a total of 180+), we expect that achieving a combined sample of 156 would be feasible. However, as the IPW approach might reduce the comparator sample due to the weighting process, this might be marginally higher than the minimum recommended sample. We therefore suggest that

[41] This can be more clearly shown in the design of difference-in-difference analysis as it compares the two groups against each other as well as before and after. By incorporating those baseline levels in the weighting, the IPW approach essentially achieves the same result as the DID in terms of controlling for the different 'starting points' of the two groups.

[42] 103 students from phase 1 and assuming a similar number can be achieved in phase 2.

responses of the non-participant survey should be improved during phase 2, while we will revisit this when the final data is available.

It is worth noting that any bigger impacts (i.e., above 0.3) would need a much smaller comparator group sample to be detected. For example, to detect a medium effect (0.5) we would need a minimum of 66 responses in the comparator group sample (assuming all the above parameters are the same and a sample of 200 accepted students is achieved).

Approach considerations

The key advantage of the IPW method over other well-known methods such as Propensity Score Matching (PSM), is that it makes use of the whole treatment group sample, instead of filtering the data to the most similar individuals. As non-parametric RD designs might need to reduce sample sizes of both groups due to comparing bandwidths, the IPW approach is worth considering as it might make use of bigger samples and thus being able to detect impact with higher statistical power. One of the key advantages of the IPW approach compared to RDD is that it can utilise almost the entire sample available, including those who did not complete their CTE exam (who would need to be removed in any RDD analysis[43]).

However, the IPW model could potentially reduce the sample size of the comparator group, which as mentioned above might be low based on current response rates. As this is a common challenge across both RD and IPW designs, we will revisit the feasibility of both when the final data from phase 2 is available.

Conclusions

Overall, we suggest that a CIE approach would be feasible to assess the impact of the Upskill in Cyber Programme in phase 2, although with a few caveats to be taken under consideration. We summarise the findings of our assessment below:

- Randomised experiments/RCTs are not feasible or appropriate for CIE of this programme for several reasons, most importantly as the selection of applicants to be accepted is not at random (nor can it be assigned at random).
- RDD and IPW methods are deemed to be the most feasible and appropriate for this design, however with caveats around data availability and sample sizes during phase 2
- Analysis using data of just one phase is most likely not possible, as both CIE approaches would need large samples to detect impact. Data from phases 1 and 2

[43] Applicants with missing data in terms of their CTE scores would not be used in any RDD, as we would not be able to determine what was their level prior to the application outcome. We would therefore not be able to allocate them above or below a cut-off, nor calculate their probability of treatment.

would most likely need to be combined to achieve a large sample needed in both approaches

- High pre-existing levels in certain outcome indicators could pose a challenge in detecting small impacts, especially considering that expected samples might be small
- Biggest gap in samples (but also most room for improvement) currently identified in the non-participant survey, as response rates in phase 1 were low, and large comparator group samples are necessary for the CIE approaches to work. We suggest working closely with government and the deliver partner to consider options on how to improve response rates in this sample, to ensure that impact can be detected with maximum achievable statistical power.