PRIVATE AND CONFIDENTIAL

RSM

Department for Science, Innovation and Technology (DSIT) Evaluation of CyberASAP

Final Report

May 2025

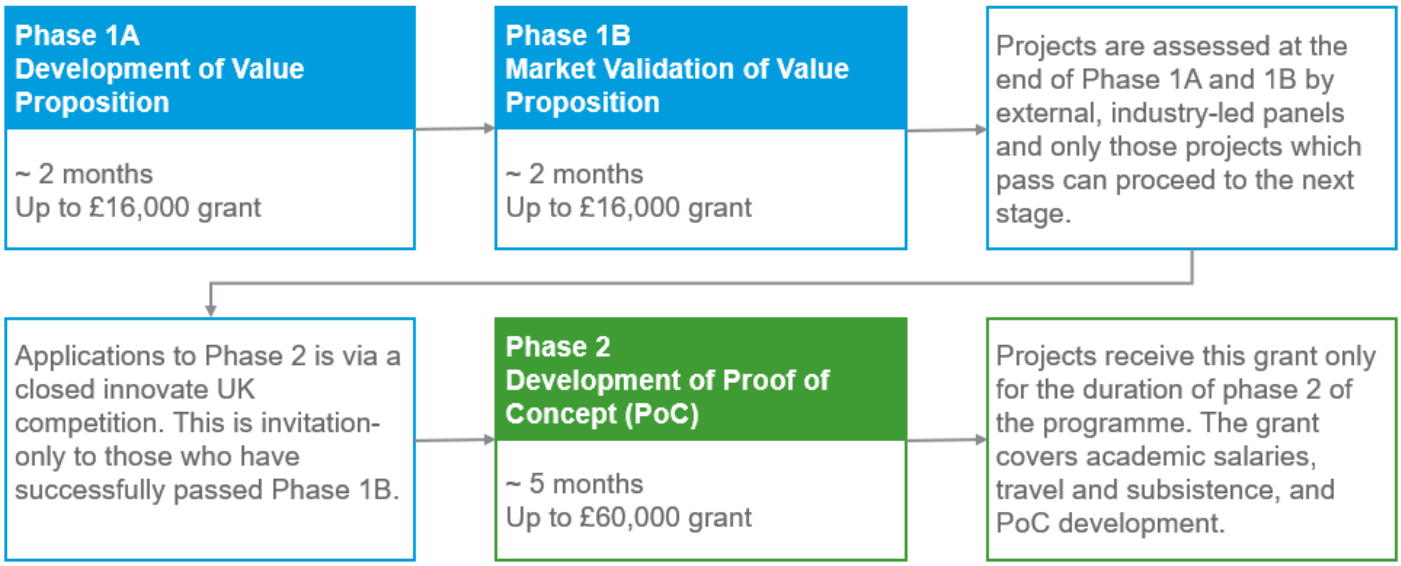
Contents

1. Executive Summary

1.1. Overview of CyberASAP

The Cyber Security Academic Start-up Accelerator (CyberASAP) programme is funded by the Department for Science, Innovation and Technology (DSIT) and delivered by Innovate UK with Plexal (Cohort 8 only). It supports the commercialisation of UK cyber security research and helps academic researchers to turn ideas into fully rolled-out commercial projects by developing the academics' entrepreneurial skills. It has two phases as shown in Figure 1.

Figure 1: CyberASAP Overview



This evaluation report relates to CyberASAP which was initially piloted in 2017/18 and has been delivered over eight years to 2024/25, with one cohort of researchers each year[1]. To date the programme has had a budget of £14,050,073 and spend of £9,793,238 (as of end of February 2025).

Conclusions and recommendations against each of the core evaluation questions are outlined below.

1.2. Process evaluation

The process evaluation assesses the implementation of CyberASAP from Year 1 to Year 8, including whether the programme was delivered as intended. It explores what worked well and less well, and for who. It identifies the external factors that influenced programme delivery and whether unexpected or unintended issues affected the delivery of the programme. Finally, it identifies what can be learned from the delivery of the programme and provides suggestions for improvements to CyberASAP that could make it more effective.

The evidence available suggests that CyberASAP has been successfully delivered as intended. Two key factors contributing to this success are the knowledge and skills of KTN/Innovate UK Business Connect, Innovate UK, Plexal, industry representatives, and trainers. These skills and knowledge led to support that participants found to be useful and of very high quality.

[1] This evaluation covers the period up to, and including, the delivery of Year 8 of the programme

KTN/Innovate UK Business Connect have successfully adapted the delivery and design of CyberASAP in collaboration with the then Department for Digital, Culture Media and Sport (DCMS) and DSIT to address feedback and potential areas for improvement since the programme's inception. Adaptations have included an increased involvement of university technology transfer officers (TTO) who can help participants navigate intellectual property (IP) requirements and university procedures, and additional engagement with alumni after they graduate from the programme.

The fast-paced delivery of the programme, including the stage-gating approach between each phase, and the skills and knowledge of those delivering it generally contributed to high levels of engagement with the content of CyberASAP.

While no unexpected or unintended issues were reported, some external factors were. Government planning cycles, which tend to favour funding for programmes delivered in one financial year, led to Innovate UK operating programme competitions at risk, before knowing whether DCMS/DSIT would fund the following year's activities. However, this has not led to any reported impacts on actual delivery to date. Despite increasing participation by university TTOs, the most frequently reported external factor affecting teams' experiences of CyberASAP was university policies and procedures. These policies and procedures can limit teams' motivation to continue to develop their projects after they graduate from CyberASAP.

There are specific areas for future development, the most important of which are: (1) additional information for potential applicants so that they can make informed decisions about whether CyberASAP is relevant for them; and (2) offering flexibility in the format and structure of pitch presentations to assessment panels, allowing for all types of ideas and researchers with diverse backgrounds to present their projects successfully. It is noteworthy that Innovate UK is likely able to address the first area for development with the new CyberASAP pathfinder, a short, free-of-charge event run since 2025.

1.3. Impact evaluation

The programme has been highly effective in enabling the academic sector to commercialise their ideas. This includes significantly raising the skills, knowledge, and confidence of academic teams to commercialise, speeding up the transition from concept to spin-out, and increasing researchers' ability to secure investment. It has also had an impact on propensity to commercialise, helping academics to embrace a pathway to impact for their research which they may not have considered before.

The programme significantly increases the probability of successful spin-out formation and accelerates the process by providing early-stage commercialisation expertise that many researchers lack. CyberASAP participants have spun out companies, licensed technology, and developed products and services. There are also examples of further knowledge and IP generation, through registration of patents and provision of outputs in open-source format.

The programme has led to improved commercial awareness, which has in turn affected how alumni think about their research through a market lens. The survey evidence has reported private sector investment, and dissemination of IP through patents and open-source software. A key additional benefit has been through licensing.

1.4. Value for money evaluation

In real terms (2024/25 prices), every £1 of programme expenditure has generated ~£3.92 of spin-out investment across Cohorts 1–8. This ratio would be expected to rise as later cohorts move toward spin-out formation and investment. Survey evidence suggests that 70%, or £2.74 per £1 expenditure, is wholly due to CyberASAP (i.e. the other 30% would have occurred anyway).

CyberASAP spin-outs have created approximately 76 net additional jobs, which are currently responsible for £8.89 million in annual GVA, after accounting for deadweight, displacement, and leakage. The ratio of annual recurring GVA to annual programme cost (£1.41m/year on average) is currently about 6.35:1. Over time, if spin-out jobs persist and grow, the cumulative economic return will improve accordingly.

The programme has used public resources in a way that maximises public value, with particularly strong results in spin-out formation and follow-on investment. It has met its targets on participation and progress while staying within budget, and accelerated progress towards commercialisation. The latter result applies even to academics who thought they might have commercialised even without CyberASAP support.

Targets for team participation and progress have been achieved without using the full allocated budget. As set out above the support is likely to be highly additional: it will benefit recipients that might not otherwise have generated commercial activity and produce novel products and services. As such, it is complementary to support aimed at existing businesses.

The programme has performed very well in terms of its economy – spending less while maintaining quality. Overall VfM could be improved by redirecting resources:

- The numbers accepted into Phase 1 could be increased, recognising that approx. 50% will drop out between Phase 1A and Phase 2; this could increase the quantity of outputs
- Resources could be proactively directed to additional targeted support for those academic teams which proceed to later phases, based on their challenges, weaknesses, and needs; this could increase the quality of the business propositions arising from the programme.

1.5. Recommendations

Process Evaluation

Recommendation 1. Innovate UK should continue to run the CyberASAP Pathfinder project so that potential applicants can understand the content of the programme and the extent to which it would be useful to them. It would be beneficial to seek feedback from CyberASAP Pathfinder participants to understand the extent to which the Pathfinder helps them decide whether to apply for CyberASAP, when to apply for CyberASAP, or make adaptations to their idea before they decide to apply to CyberASAP. Doing this will help ensure that the Pathfinder is useful to applicants so that academics can make the most of CyberASAP itself.

Recommendation 2. Participants should be required to book up to three events following the networking training to put what they learned into practice. After this, they should report back to Innovate UK and the trainer. This would ensure that participants start to build their network and put what they learn into practice while they are still part of the programme.

Recommendation 3. DSIT and Innovate UK should formulate more specific challenges for the industry challenge-led cohort. Specific business challenges could be more effective in achieving the desired outcomes, including projects with specific real-world applications, of CyberASAP than general themes. The challenges formulated for the industry challenge-led cohort in Year 8 were broad, representing themes such as cybersecurity supply chains.

Recommendation 4. DSIT, Innovate UK should consider whether participants can have more flexibility in the format and structure of their pitches to assessment panels, including for instance written submissions in addition to the presentation. Flexibility could allow teams to focus more on the strengths of their ideas while considering that some participants do not have English as their first language. Implementing this

recommendation will require Innovate UK to support assessors with guidance on how to consistently score pitches despite varying format and structure.

Recommendation 5. Assessment panels in between phases could be strengthened through the inclusion of further technologically knowledgeable people such as Chief Information Security Officers, who can give reasoned feedback on the applicability and relevance of ideas to current challenges. Innovate UK would need to work with industry to encourage CISOs to take part in panels.

Recommendation 6. So that DSIT can assess the achievement of key outputs and outcomes in-year, rather than after the conclusion of each year of the programme, or through evaluations such as this one, monthly reporting should include further key outputs and outcomes of the programme, including the number of proof-of-concept demonstrators, new patents and technologies, and market validated value propositions.

Impact Evaluation

Recommendation 7: CyberASAP should continue to provide comprehensive, high-quality commercialisation training to ensure participants are well-equipped to refine their ideas into commercially viable products and are well-prepared to present to investors.

Recommendation 8: Allied to Recommendation 7, CyberASAP should investigate expert mentoring in niche technology areas such as deep tech to improve the quality of training in these.

Recommendation 9: CyberASAP should implement longer-term support mechanisms to support business survival and growth post-programme participation. The impact on survival rates is hardest to evidence at this point, so support should be forward-looking to head off any problems companies may face, and should be customised for individual sectors, and additional to support provided by universities and their TTOs.

Value for Money Evaluation

Recommendation 10: The programme demonstrates good economy through budget management and minimising overheads. However, CyberASAP should improve its effectiveness and efficiency by securing more tailored mentor expertise to support sectors such as deep tech. This would improve quality of outputs by directing bespoke training towards demos and final pitches in niche sectors, which were mentioned as a relative weakness, and could also be deployed towards longer-term support.

Recommendation 11: The current level of underspend per cohort should be investigated – this could be deployed towards the extra support mentioned in Recommendations 8 and 10, or towards recruiting more academics per cohort if there is demand for this among high-quality applicants.

Recommendation 12: Building on the progress in regional reach and the increase in female principal investigators since Cohort 1, CyberASAP should consolidate its equity gains by systematically recording and reporting the gender and ethnicity of all team members (not just the PI) at each phase-gate, using those data to fine-tune outreach so that improvements are transparent, evidence-led, and firmly linked to the wider talent pipeline.

2. Terms of Reference and Methodology

2.1. Introduction

The Department for Science, Innovation and Technology (DSIT) appointed RSM UK Consulting LLP to evaluate the Cyber Academic Start-up Accelerator Programme (CyberASAP) Years 1 to 8 (2017 to 2025).

This involves a process evaluation, impact evaluation, and economic evaluation. The process evaluation seeks to understand what has worked well and less well in the design and delivery of the programme and makes recommendations for changes to the delivery process. The impact evaluation seeks to understand what the programme has achieved, and the economic evaluation provides evidence on the programme's value for money (VfM).

2.2. Terms of reference/evaluation aims

The evaluation has the following objectives:

- Determine how CyberASAP has performed since it was first launched in 2016. It should assess the delivery of CyberASAP and provide evidence of the effectiveness and efficiency of the programme.
- Review the current in-train year of the programme.

These objectives will be met by answering the key evaluation questions in Appendix A.

2.3. Methodology

To answer the process, impact, and VfM evaluation questions, this report draws on findings from monitoring data, participant survey data, annual reports, impact reports, and other reports, interviews with participants, delivery leads, and stakeholders, and published data. Details of each component of the evaluation are provided in the following three sub-sections.

2.3.1 Process evaluation

The process evaluation examines the extent to which CyberASAP was delivered as intended, identifies what worked well or less well, uncovers any unexpected issues, and assesses the influence of external factors on the programme's expected outcomes. Additionally, it derives lessons from the different delivery methods and suggests potential improvements for greater effectiveness. The process evaluation draws on monitoring data, participant survey data, annual reports, impact reports, and other reports, and interviews with participants, delivery leads, and stakeholders. These questions are answered through descriptive analysis and qualitative framework analysis.

2.3.2 Impact evaluation

The impact evaluation assesses the effectiveness of CyberASAP in enabling the academic sector to commercialise ideas, achieving expected outcomes within budget, addressing post-graduation challenges, and influencing academic culture and behaviour. It also evaluates CyberASAP's success in bringing research outputs to market, any additional benefits, differences in outcomes across university types, and its impact on the UK economy.

The impact evaluation draws on participant survey data, annual reports, impact reports and other reports, interviews with participants, delivery leads, and stakeholders, and published data (including Beauhurst, Office for National Statistics (ONS), and ASHE (Annual Survey of Hours and Earnings)).

The impact evaluation questions are answered through descriptive analysis, qualitative framework analysis, contribution analysis, process tracing, and Bayesian Updating, which are described below:

Contribution analysis: We tested the following contribution claims by mapping data against each claim to evaluate both the strength of the contribution and the robustness of the supporting evidence:

1. CyberASAP contributes to the skills and knowledge needed for academics to turn an idea into a viable product.

2. CyberASAP contributes to the skills, confidence and knowledge needed for academics to spin out a company.

3. Participating in CyberASAP contributes to attracting new investment from private and/or public sources.

4. Participating in CyberASAP contributes to high survival rates of companies that spun out of university research.

Process tracing: We used process tracing to test whether the hypothesised causal mechanisms explain the outcomes, thereby allowing for the examination of contribution claims. We used four process tracing tests ("straw in the wind", "hoop", "smoking gun", and "double decisive") to help assess the qualitative strength of the evidence and determine the extent to which the support given to researchers through CyberASAP has contributed to the various outcomes and impacts achieved. Further descriptions of the process tracing tests are available in Section 5.4. Collectively, these tests identify whether the causal mechanisms described in the contribution claims are sufficient and/or necessary to explain the outcomes.

Bayesian Updating: We used Bayesian Updating to quantify our confidence in CyberASAP's impact by assessing the strength of evidence supporting the contribution claims and alternative hypotheses. We started with a prior probability, which was adjusted as new evidence was incorporated, resulting in a posterior probability that reflected the updated confidence level.

2.3.3 Value for Money (VfM) assessment

The economic VfM assessment evaluates how the economic value of the benefits attributed to CyberASAP compare with the programme costs. This assessment draws on all evidence gathered through the evaluation. We have calculated a Return on Investment (ROI) across all cohorts, in compliance with His Majesty's Treasury (HMT) Green Book[2] and including:

- Estimates of monetisable benefits – financial gains or savings directly attributable to CyberASAP that can be measured in monetary terms.

- Deadweight, based on survey data from participants who started a company after participating in CyberASAP, indicates whether they would have started a company without CyberASAP's intervention.

- Displacement and leakage estimates from survey responses or secondary economic data, showing the extent to which any benefits replace or reduce outcomes elsewhere (displacement), or flow outside the intended target group or region (leakage).

This has been supplemented with analysis of VfM using the National Audit Office 4Es framework[3:] economy, efficiency, effectiveness, and equity.

[2] The Green Book (2022) - GOV.UK (Accessed 25/02/2025).
[3] Successful commissioning toolkit Assessing value for money - National Audit Office (NAO) (Accessed 25/02/2025).

2.3.4 Limitations

The evaluation has the following limitations:

Low survey response rate: The reliability and generalisability of findings are affected by low survey response rates and a limited number of interview data points, which weakens the evidence of causal links.

- **Mitigation:** We have access to previous CyberASAP evaluation surveys with higher response rates. Where the findings in the new surveys are similar to those in the previous surveys, we can likely conclude that the impact on the reliability of the findings is limited.

Availability of benchmarking comparator country data: Despite identifying useful international comparison programmes and communicating with their representatives via email or interview, two of the comparator programmes are ongoing and have yet to collect much data on their outcomes and impacts. Therefore, our reporting on some aspects is limited and restricts the ability to benchmark CyberASAP's performance against international standards fully.

Skewed startup outcome distributions: Due to the nature of technology start-ups, their outcomes often exhibit skewed distributions, meaning a small number of start-ups achieve very high levels of success (e.g., significant business turnover, securing substantial investment), while the majority experience more modest outcomes. This skewness is typical in the start-up ecosystem, where a few high-performing companies drive most of the overall success and therefore could be present within our evaluation.

3. Rationale and Programme Overview

This section details the strategy, delivery context, and rationale for CyberASAP, as well as providing an overview of other programmes in this sector.

3.1. Policy context

CyberASAP is expected to contribute to several key national strategies, as set out below.

Table 1: Strategic context

Strategy	How CyberASAP is expected to contribute
National Cyber Strategy 2022[4] (and accompanying latest annual report 2022-23)	CyberASAP is expected to play a key role in advancing this strategy by bridging the gap between academia and commercial application, fostering growth and innovation within the UK cyber sector, and improving skills and diversity of the cyber workforce. Additionally, CyberASAP supports the UK's leadership in cyber technologies, ensuring the UK remains at the forefront of technological advancements and is '*more successful at translating research into innovation and new companies in the areas of technology most vital to our cyber power*'.
Government Cyber Security Strategy (2022 – 2030)[5]	This strategy focuses on building a cyber-resilient public sector by improving governance, managing, and protecting against risks, and developing the necessary skills to meet these aims. CyberASAP aligns with the strategy's objectives by translating cutting-edge research into practical applications to address current and emerging cyber threats faced by government, improving resilience, and providing training and support to researchers.
UK Research and Innovation (UKRI) Strategy (2022 – 2027)[6]	CyberASAP is expected to contribute to UKRI's strategy through delivering skills, finance, and collaboration opportunities needed to boost private sector investment in cybersecurity innovation. It helps researchers develop entrepreneurial skills and investment sources. CyberASAP accelerates the commercialisation of cybersecurity research, fostering collaboration and co-investment between businesses, universities, and the wider research base which increases adoption and diffusion of cybersecurity innovations across the UK. It also supports the development and commercialisation of advanced cybersecurity technologies, securing a competitive advantage for the UK.
The UK Science and Technology Framework[7] (last updated 2024)[8]	CyberASAP aligns with the framework's goals by: ▪ Increasing the commercialisation of academic research in cybersecurity, in alignment with the framework's aim of catalysing private sector R&D and boosting innovation activity. ▪ Providing training and mentoring to academics in commercialisation and business management skills. ▪ Ensuring early-stage capital for cybersecurity innovation and facilitating domestic investor participation, strengthening the pipeline of spin-outs, and easing the path to public listing.

[4] National Cyber Strategy (Accessed 04/02/2025).
[5] Government Cyber Security Strategy 2022–2030 (Accessed 04/02/2025).
[6] UKRI Strategy 2022-2027 (Accessed 04/02/2025).
[7] The UK Science and Technology Framework: taking a systems approach to UK science and technology (Accessed 04/02/2025).
[8] Science & Technology Framework - Update on progress (Accessed 04/02/2025).

Strategy	How CyberASAP is expected to contribute
DSIT UK Innovation Strategy (last update 2023)[9]	CyberASAP is expected to play a role in advancing DSIT's strategy by bridging the gap between academic research and commercial application. It provides funding, mentoring, and support to translate cybersecurity ideas into commercial products. This aligns with the strategy's goals of increasing public R&D investment and simplifying financial support access. CyberASAP nurtures talent and promotes academia-industry collaboration, contributing to making the UK a leader in cybersecurity innovation and a global innovation hub by 2035.
DSIT National Data Strategy (last updated 2022)	CyberASAP supports this strategy by helping researchers transform their ideas into market-ready products and services, which in turn is expected to develop advanced cybersecurity solutions. These innovations will be key to enhancing the UK's ability to protect its data infrastructure, ensuring that data is accessible, usable, and secure.
Independent Review of University Spin Out Companies[10]	CyberASAP addresses the review's key findings by providing proof-of-concept funding and aligning with recommendations for increased government support for concepts prior to spinning out. It offers training for academics to become entrepreneurs and commercialise their research. CyberASAP improves the provision of funds for academia-industry movement and provides opportunities for academics to access high-quality entrepreneurship training and work within local spin-outs and with venture capital firms or Technology Transfer Offices (TTOs).

3.2. The UK cyber security sector growth and innovation space

The UK cyber security sector is a vital and growing part of the UK economy, as detailed in the UK Cyber Security Sectoral Analysis[11] published in 2025. This is shown by:

- Approximately 67,299 Full Time Equivalents (FTEs) are employed in the cyber security sector (an 11% increase from the previous year, higher than the 5% growth rate seen in the previous study). Most cyber security employment (65%) is concentrated within large firms of over 250 employees.
- The sector's estimated revenue is £13.2 billion, a 12% increase from the previous year's study.
- The total Gross Value Added (GVA) of the sector reached £7.8 billion, an increase of 21% from the previous year. GVA per employee also increased from £106,300 to £116,200 (8%).
- For the first time, the highest proportion of external investment was in the North West (49%) with six deals to the value of £102 million. This marks a shift away from the historical focus on the South East and London.

However, the sector is facing some challenges. 2024 was a stable yet challenging year for UK cyber security investment. The 2025 UK Cyber Security Sectoral Analysis notes that investment in cyber security firms decreased to approximately £206 million across 59 deals, down from the record figures of £814 million in 2020 and £1.013 billion in 2021[12]. These record figures were likely due to favourable wider macroeconomic conditions, including low interest rates and high demand for technology investments. The 2024 investment level remains relatively stable compared with 2022 and 2023.

While total investment has decreased, the geographical distribution within the UK has diversified. Investment outside London and the South East of England grew to nearly half of the total (49%), up from

[9] UK Innovation Strategy: leading the future by creating it (accessible webpage) - GOV.UK (Accessed 04/02/2025).
[10] Independent Review of University Spin-out Companies (Accessed 05/02/2025).
[11] Cyber security sectoral analysis 2025 - GOV.UK (Accessed 27/03/2025).
[12] This figure is for cybersecurity-dedicated firms and excludes investment in diversified firms.

35% in 2023 and 25% in 2022. Increasing regional investment access is a key objective of the national cyber security strategy.

The UK is recognised as a leader in cyber security research, with contributions from 21 Academic Centres of Excellence in Cyber security Research (ACE-CSR)13, four Engineering and Physical Sciences Research Council – National Cyber Security Centre (NCSC) Research Institutes14, four Centres for Doctoral Training15, and the Centre for Secure Information Technologies (CSIT)16.

There are several challenges currently facing the cyber security sector and the innovation landscape:

- **Regional divide:** Despite increased investment outside London and the South East of England, this was almost entirely within the North West. There are still seven UK regions (East Midlands, Northern Ireland, North East, Scotland, West Midlands, East of England, and Wales) generating less than 1% of the total UK cyber security investment each, highlighting sustained disparity with respect to large scale investments.
- **Economic climate:** The UK economic climate has posed challenges for the cyber security sector, with investment in 2023 and 2024 notably lower than the record figures of 2020 and 2021. This decline is attributed to rising interest rates and revised firm-level valuations, which have reduced external investment across sectors.
- **Technical skills shortage:** The UK cybersecurity sector faces a significant shortage of candidates with the necessary technical skills. According to the survey, 47% of businesses report a lack of candidates with the required technical cybersecurity skills, impacting their ability to effectively address cybersecurity threats and vulnerabilities.
- **Difficulty commercialising academic research into cyber security products and services:** There are many barriers to commercialising academic research into cyber security products and services, including access to funding, ability to dedicate time to market research and validation, and balancing the demands of teaching, research, and commercial activity[17]. 33% of surveyed businesses report a lack of employees with non-technical skills (e.g., communication, management, sales, and marketing), and 32% report a shortage of such candidates in the labour market[18], which is likely to contribute to this challenge.
- **Challenges for the UK innovation landscape:** The DSIT UK Innovation Strategy[19], highlights the challenges the UK innovation landscape faces related to accessing finance and experiencing regulatory obstacles. Innovators experience difficulties obtaining finance, particularly in the early stages of development, and regulations are not agile enough to keep up with technological advancements.

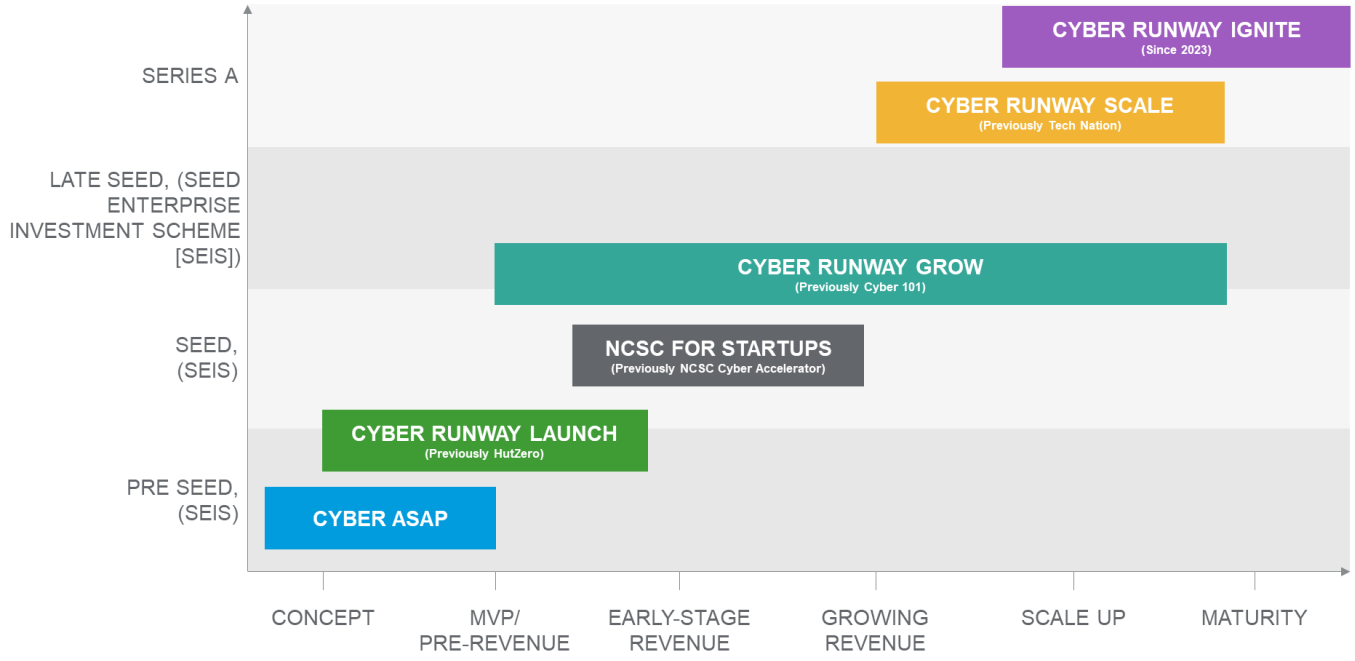
CyberASAP exists to bridge the gap between academic research and commercialisation, addressing the unique challenges faced by academics in bringing their cyber security innovations to market. CyberASAP aims to address the challenges above through supporting projects across the UK and encouraging diversity by promoting inclusive participation.

[13] Academic Centres of Excellence in Cyber Security Research - NCSC.GOV.UK (Accessed 20/02/2025).
[14] Research institutes - NCSC.GOV.UK (Accessed 20/02/2025).
[15] Centres for Doctoral Training – EPSRC – UKRI (Accessed 20/02/2025).
[16] CSIT | Queen's University Belfast (Accessed 20/02/2025).
[17] Microsoft Word - Short Commercialisation Piece.docx (Accessed 21/02/2025).
[18] Cyber security sectoral analysis 2025 - GOV.UK (Accessed 27/03/2025).
[19] UK Innovation Strategy: leading the future by creating it (accessible webpage) - GOV.UK (Accessed 20/02/2025).

3.3. Mapping of other programmes

CyberASAP is part of a wider ecosystem of cyber security growth and innovation programmes across different stages of the 'innovation pathway', as illustrated in Figure 2.

Figure 2: Cyber security growth and innovation programmes



CyberASAP is the first 'stage' in the innovation pathway focused on pre-seed and proof of concept ideas. It supports the commercialisation of UK cyber security research into fully rolled-out commercial projects. It is complemented or followed by programmes that support companies at different stages of the lifecycle to:

- **Launch:** To support the establishment of new companies in the sector by helping to transform early-stage cyber security ideas into workable proposals and potential new businesses (programme: Cyber Runway Launch).
- **Grow:** To support existing SMEs in the early and growth stages of the life cycle to improve the survival rate of early-stage cyber businesses (programmes: NCSC for Startups and Cyber Runway Grow).
- **Scale:** To support cyber security scale-ups to address barriers to growth (programmes: Cyber Runway Scale and Ignite).

There are several programmes available to support innovation within the UK's wider cyber security ecosystem. However, there are no other initiatives focused primarily on the pre-seed, concept stage. While Cyber Runway Launch aims to support the establishment of new companies in the sector, CyberASAP's focus is on addressing the challenges faced by academics in the commercialisation of research.

3.4. Programme overview and funding

This section provides details on the background of CyberASAP, its evolution over the eight cohorts from 2017 and 2025, and how the programme was delivered and funded.

3.4.1 Background to the programme

CyberASAP was initially set up as a pilot in 2017 based on research by the Knowledge Transfer Network (KTN) into barriers for the commercialisation of research in cyber security. The programme's development is outlined in the following table.

Table 2: CyberASAP development

Year	Summary
Year 1 (2017)	The initial pilot was funded by Innovate UK and delivered by SetSquared. It incorporated the Innovation to Commercialisation of University Research (ICURe) model for training. KTN provided additional business training to support projects in developing a Minimum Viable Product (MVP) and held a showcase/demo day in October 2017.
Year 2 (Programme Design, 2017 and delivery 2018-19)	KTN, working with the then Department for Digital, Culture Media and Sport (DCMS) and Innovate UK, redesigned the programme based on feedback from teams, DCMS, and Innovate UK through the Year 1 pilot programme. The new programme split the activities into commercial proposition development stages, with an external selection panel of industry experts assessing projects before advancing to the next stage. In addition, a range of personal development skills were introduced to the programme. The obligation to spin out/form a company at the development grant stage was removed to provide more support and development time.
Year 3-6 (Delivered over each financial year 2019-2023)	The programme further evolved based on feedback from cohorts, alumni, and industry. In Year 5, it was opened to participants of the Security of Digital Technology at the Periphery (SDTaP) programme, with funding from an Innovate UK budget (UKRI Strategic Partnerships Fund) and shared running costs with DCMS. The content remained the same for both DCMS and SDTaP projects.
Year 7 (2023-24)	The responsibility for delivering CyberASAP transitioned from DCMS to DSIT in February 2023, consolidating efforts in advancing technology and innovation under one department. Year 7 continued in the same manner as previous years of delivery.
Year 8 (Delivered over financial year 2024-25)	Following a review, DSIT introduced a thematic call for academic projects addressing market failures in cyber security, alongside the open call. Year 8 comprised two parallel cohorts: one open to any cyber security research project and another focused on specific industry challenges. While most programme content remained the same for both cohorts, the challenge-led cohort received targeted support from Plexal, the industry-facing delivery partner. Selected industry challenges included AI model security, software supply chain security, and Industrial Internet of Things (IIOT) or Operational Technology (OT) security.

3.4.2 Programme delivery and aims/objectives

CyberASAP is designed to support the objectives of the Technology Advantage Pillar in the UK's National Cyber Strategy 2022, specifically Objective 2: 'Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace'[20]. It also supports the government's mission to Kickstart Economic Growth by supporting the formation of spin-out companies.

The programme consists of the two phases with the following key objectives:

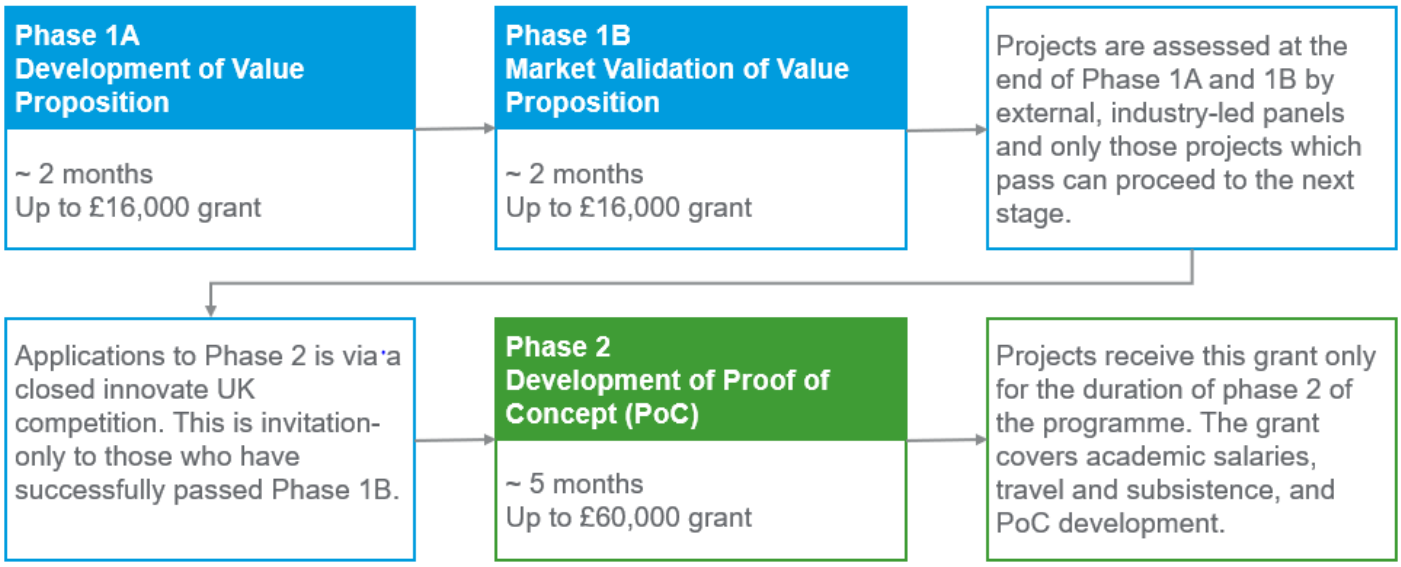
- **Phase 1A – Development of Value Proposition:** Participants test and refine their value proposition throughout the 6–8-week phase of the programme, ensuring that the product/service has an addressable market.

[20] For more detail on this Pillar and the other four strategic Pillars, see the National Cyber Strategy 2022 here: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 (Accessed 20/02/2025).

- **Phase 1B – Market validation of Value Proposition:** The 6-8-week phase enables participants to validate their value proposition through engagement with prospective market clients. They also receive business support to help progress towards a business.
- **Phase 2 – Development of Proof of Concept (PoC):** This phase enables participants to build their Proof of Concept from their university base.

Participants take part in several mandatory activities during each phase and a Demo Day at the end of Phase 2. The programme lasts twelve months and provides academics with expert knowledge, skills, and support via bootcamps, training, tools, mentoring, peer to peer learning, and industry showcases.

Figure 3: CyberASAP overview



4. Process Evaluation

The process evaluation in this section assesses the implementation of CyberASAP from Year 1 to Year 8, including whether the programme was delivered as intended. It explores what worked well and less well, and for who. It identifies the external factors that influenced programme delivery and whether unexpected or unintended issues affected the delivery of the programme. Finally, it identifies what can be learned from the delivery of the programme and provides suggestions for improvements to CyberASAP that could make it more effective. To do so, this section draws on management and monitoring information for Years 6 to 8, previous evaluation and annual/end of year reports from Year 1 onwards, interviews with programme stakeholders and participants in Years 6 to 8, and surveys of participants in Years 6 to 8.

4.1. Summary of key findings

The evidence available suggests that CyberASAP has been successfully delivered as intended. Two key factors contributing to this success are the knowledge and skills of KTN, Innovate UK, Plexal, industry representatives, and trainers. These skills and knowledge led to support that participants found to be useful and of very high quality. Furthermore, KTN/Innovate UK Business Connect have adapted the delivery and design of CyberASAP in collaboration with DCMS/DSIT to address feedback and potential areas for improvement since the programme's inception. Adaptations have included an increased involvement of university TTOs, who can help participants navigate IP requirements and university procedures, and additional engagement with alumni after they graduate the programme.

There are specific areas for future development, the most important of which are: (1) additional information for potential applicants so that they can make informed decisions about whether CyberASAP is relevant for them; and (2) offering flexibility in the format and structure of pitch presentations to assessment panels, allowing for all types of ideas and researchers with diverse backgrounds to present their projects successfully. It is noteworthy that Innovate UK is likely able to address the first area for development with the new CyberASAP pathfinder, a short, free-of-charge event run since 2025. However, this process evaluation could not yet comment on the extent to which the Pathfinder is likely to provide potential applicants with all the information they need.

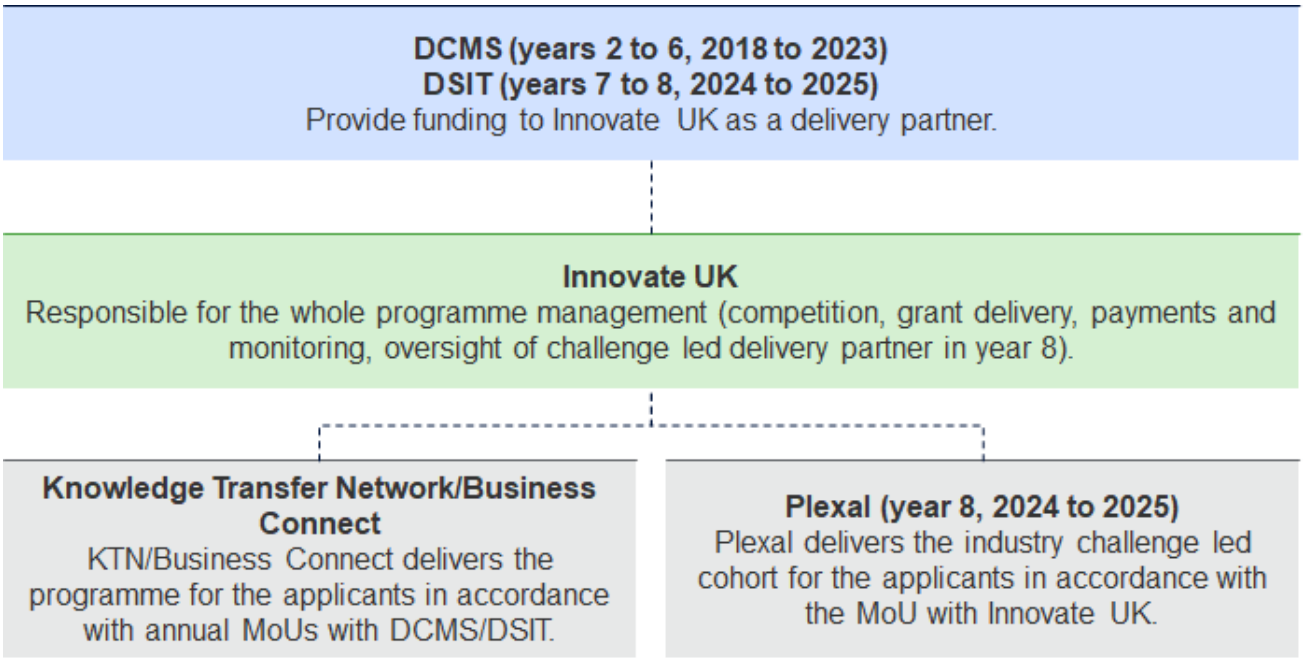
4.2. CyberASAP governance structure

In Year 1 (2017) the delivery partners were:

- Phase 1: SetSquared (as part of the ICURe programme) – focused on delivery of the support programme and management, and funding to university teams.
- Phase 2: SetSquared (as part of the ICURe programme) – focused on management and payment of funding university teams.
- Phase 2: KTN – focused on delivery of the business support programme.

The governance structure for CyberASAP in Years 2 to 8 is outlined in Figure 4.

Figure 4: CyberASAP governance structure (Years 2 to 8, 2018 to 2025)



Sources: DSIT (2023) Evaluation of the Cyber Security Academic Startup Accelerator, Memoranda of Understanding between DSIT / DCMS and Innovate UK and between Innovate UK and Plexal

4.2.1 Roles and responsibilities

The following table provides further detail on the roles and responsibilities of each organisation, from Year 2 onwards. In Year 1, the SetSquared partnership delivered a pilot programme funded by Innovate UK.

Table 3: Roles and responsibilities

Organisation	Roles and responsibilities
DCMS/DSIT	Management of: • Funding – provides funding to InnovateUK for administrative costs, KTN/Innovate UK Business Connect costs, Plexal costs, grants, and delivery costs; and • Attendance at events in an advisory capacity.
Innovate UK	Management of: • Funding – for the delivery partners, KTN and Plexal, who deliver the programme to the academic teams; and • Funding – for the academic teams through their universities via standard Innovate UK grant-funded competitions. Project management activities: • In accordance with UKRI-Innovate UK's standard operational procedures, and its corporate policies; • Reviewing progress of the programme at regular intervals with DCMS/DSIT; • Meeting quarterly and ad-hoc as needed with DCMS/DSIT; • Acting as an escalation point for urgent or contentious matters; and • Ensuring that programme management includes sufficient focus on the evaluation of benefit forecasts, with appropriate teams and resource consulted to deliver an effective evaluation strategy as part of the management of the programme.

Organisation	Roles and responsibilities
	• Contracting – with KTN and Plexal to deliver CyberASAP. • Reporting – providing DCMS/DSIT with monthly financial and monitoring reports. • Marketing – assisting DCMS/DSIT with marketing by encouraging UK universities to apply to CyberASAP.
KTN/Innovate UK Business Connect	Innovate UK contract KTN/Innovate UK Business Connect to deliver the programme content. They are responsible for devising and delivering the programme, either directly or through third party trainers and stakeholders, via: • Bootcamps; • Training; • Tools; • Mentoring; • University technology transfer officer (TTO) and commercialisation office briefings; • Investor meetings and other events; • Peer to peer learning; and • An industry showcase (demo day). KTN/Innovate UK Business Connect have delivered the programme since Year 2, taking over the role from the SetSquared partnership after the first two phases of Year 1 were completed as part of the ICURe programme. KTN/Innovate UK Business Connect provides final reports at the end of each year, summarising the activities and results achieved. KTN/Innovate UK Business Connect also deliver alumni engagement activities.
Plexal	Innovate UK contract Plexal to deliver additional programme content for the industry challenge-led cohort in Year 8. They are responsible for devising and delivering the programme via: • Bootcamps; • Training; • Tools; • Mentoring; Investor meetings and other events; • Peer to peer learning; • An industry showcase (demo day); and • A graduation event (delivered as part of a House of Lords event).

Sources: DSIT (2023) Evaluation of the Cyber Security Academic Startup Accelerator, Memoranda of Understanding between DSIT / DCMS and Innovate UK and between Innovate UK and Plexal.

4.3. Programme delivery

The following sections discuss the design and delivery of the programme. They also discuss how the programme was communicated and how the application process worked. The section proceeds with findings about the support provided to participants, their experiences of monitoring and reporting requirements, and how external factors influenced the programme. It concludes with learnings about the programme.

4.3.1 Key phases / stages

4.3.1.1 Design

The programme was initially designed collaboratively by DCMS, Innovate UK, and KTN, to overcome challenges faced by academics when attempting to commercialise their research. Over time, ideas for additions or changes (e.g., size of grant for Phase 2 which has been gradually reduced from £100,000 to

£60,000 based on experience from delivery) have come from different stakeholders and are discussed collaboratively ahead of confirmation of the following year's activities.

Industry representatives on assessment panels, university TTOs, and trainers had almost exclusively positive views about the design of CyberASAP. Commonly cited factors included CyberASAP's stage-gated approach and the involvement of cybersecurity sector expertise in aspects of the programme such as assessment panels.

These stakeholders also stressed the value of a programme that is focused purely on cyber security. They felt it is important the UK brings together and supports academics working in this field to address urgent security challenges and noted that CyberASAP does this. They felt it would be beneficial to have more industry or sector focused commercialisation programmes like CyberASAP in other technology areas.

4.3.1.2 Participant satisfaction with the design

Year 6 to 8 participant survey respondents indicated very high satisfaction with the structure of the programme and its individual phases, ranging from 96% to 100%:

- 100% of respondents (n=47) were very satisfied (66%) or satisfied (34%) with the Value Proposition development.
- 96% of respondents (n=46) were very satisfied (65%) or satisfied (30%) with the Market Validation development.
- 96% of respondents (n=27) were very satisfied (59%) or satisfied (37%) with the Proof of Concept (PoC) development.

This is in line with high satisfaction levels with these aspects of CyberASAP among Year 1 to 5 participants[21].

4.3.1.3 Delivery

In Years 2 to 8, there were a single call for applications, a single competition, and a single intake of projects per year. Further detail about delivery is listed below.

- In Year 2 (2018/19), the competition for applicants opened in January and the programme commenced in February, running until the following January.
- Every year since Year 3 (2019), projects have been delivered within one single financial year, starting in April or May and concluding the following February or March. Competitions for applicants usually open in February and close in March, prior to delivery start dates in April or May of the same calendar year.
- There have not been any substantial slippages or delays to the delivery of planned activities. In Year 5 (2021), DCMS had to await the outcome of the spending review before proceeding with Year 6. This led to a one-month delay of the Year 6 programme confirmation[22]. A similar one-month delay occurred in Year 6 for the confirmation of the seventh year of the programme[23].

[21] See DSIT (2023) Evaluation of the Cyber Security Academic Startup Accelerator (available online: https://www.gov.uk/government/publications/evaluation-of-the-cyber-security-academic-startup-accelerator/evaluation-of-the-cyber-security-academic-startup-accelerator#cyberasap-impact-evaluation---performance, accessed 18/03/2025).
[22] See DSIT (2023) Evaluation of the Cyber Security Academic Startup Accelerator (available online: https://www.gov.uk/government/publications/evaluation-of-the-cyber-security-academic-startup-accelerator/evaluation-of-the-cyber-security-academic-startup-accelerator#cyberasap-impact-evaluation---performance, accessed 18/03/2025).
[23] Year 6, Final Logframe; Year 7, March 2023 Logframe; Year 8, December 2024 Logframe. Year 8 is still in progress.

The following figure shows how many projects started and progressed through the phases of CyberASAP.

Figure 5: Participants for each phase of CyberASAP 2017 to 2025

Source: CyberASAP logframes, end of year reports, information provided by DSIT to RSM UK Consulting LLP

4.3.1.4 Satisfaction with delivery

Year 6 to 8 participants were asked how satisfied they were that the amount of time and resources spent on the programme was matched by benefits to their projects. Satisfaction with these aspects was high, ranging from 89% to 96% (n=47):

- 96% of respondents were very satisfied (72%) or satisfied (23%) with the amount of other people's time they needed. One respondent each was either neither satisfied nor dissatisfied (2%) or very dissatisfied (2%).
- 91% of respondents were very satisfied (55%) or satisfied (36%) with the amount of money required to take part. Three respondents (6%) were neither satisfied nor dissatisfied and one (2%) was very dissatisfied.

- 89% of respondents were very satisfied (60%) or satisfied (30%) with the amount of their own time needed. Three (6%) were neither satisfied nor dissatisfied and one each were dissatisfied (2%) or very dissatisfied (2%).

In interviews, a small number of academics participating in Years 6 to 8 noted that they were surprised by the amount of time they needed to commit during CyberASAP. Prior engagement of potential applicants through the new CyberASAP Pathfinder[24], a short, free programme for academics interested in CyberASAP, is likely to help academics to understand the amount of time and work required for the programme. Nonetheless, the positive survey feedback suggests the time and resource requirements were appropriate.

Examples of areas for improvement cited by most interviewees included delivering activities before Phase 1A aimed at encouraging potential project applicants to refine their ideas and an additional focus on engaging with programme alumni. At the time of writing this report, the delivery partners were addressing both areas through a CyberASAP Pathfinder and additional alumni tracking and events.

Satisfaction with programme delivery and the structure of the programme in previous years was also high[25].

4.3.2 Communication and promotion

Since Year 2, KTN/Innovate UK Business Connect communicated and promoted the programme in several ways, including via:

- A social media strategy
- X (formerly Twitter) and LinkedIn accounts and the Innovate UK KTN and Innovate UK websites.
- Use of DCMS/DSIT, Innovate UK, KTN/Innovate UK Business Connect and Cyber Exchange networks and contacts.
- The in-house KTP advisors who support the KTP programme (a KTP connects universities and UK businesses meaning the KTP advisors cover all UK universities).
- A dedicated communications lead and KTN/Innovate UK Business Connect communications team.
- A dedicated events lead who worked with the communications lead and the core delivery team to ensure that all activities were promoted and supported (this included the promotion of competition and wider events).

KTN/Innovate UK Business Connect maintains a year-round general 'expression of interest' in the programme which is used to promote the competition when it opens. These activities made the programme '*very well publicised*' already in 2017, according to one TTO.

From Year 3 of the programme onwards, KTN introduced weekly online drop-ins for participants and alumni, as well as an alumni newsletter highlighting opportunities for grants, investment, event participation, and new programmes. KTN/Innovate UK Business Connect also introduced an alumni tracking programme to facilitate and encourage alumni engagement. Using underspends from previous years, Innovate UK provided alumni with additional funding to support marketing activities aimed at increasing awareness of the products and services developed through CyberASAP participation. Innovate UK also organised an event for alumni ahead of the demo day that concludes Phase 2 of the Year 8 programme.

[24] See: https://iuk-business-connect.org.uk/opportunities/cyberasap-pathfinder-2025/ (accessed 04/03/2025).
[25] See DSIT (2023) Evaluation of the Cyber Security Academic Startup Accelerator (available online: https://www.gov.uk/government/publications/evaluation-of-the-cyber-security-academic-startup-accelerator/evaluation-of-the-cyber-security-academic-startup-accelerator#cyberasap-impact-evaluation---performance, accessed 29/01/2025).

These additional alumni activities reflected a desire from delivery partners to do more to follow up with and engage alumni after their graduation. Training providers noted this ongoing engagement positively, as it exposed current teams to the successes and challenges that previous teams encountered both during and after participation in CyberASAP.

Plexal undertook promotional activities to raise awareness of the industry challenge-led cohort in Year 8. This included:

- A dedicated website[26].
- An online briefing event.
- LinkedIn accounts.
- Use of existing networks such as the Home Office's Accelerated Capability Environment researcher network and the Academic Centres of Excellence in Cyber Security Research network recognised by the National Cyber Security Centre.

For Years 7 and 8, Innovate UK introduced a short pathfinder project that aimed to engage potential academic projects before they decided whether to apply for CyberASAP.

4.3.2.1 Participant and delivery partner views on communication and promotion

Participant survey responses (n=47) for Years 6 to 8 results indicate that:

- The most common route through which participants in Years 6, 7 and 8 were made aware of CyberASAP was through other researchers (43% of respondents).
- Other common sources included other university sources generally (excluding TTOs, 23%) and Innovate UK or Innovate UK (21%).
- Seven (15%) participants heard about CyberASAP through their university TTO. It is notable that the proportion who heard about CyberASAP through their TTO is higher for participants who progressed to Phase 2 of Year 8 of the programme (n=14, 29%) than for all participants in Years 6, 7 and 8.
- Only three respondents each (6%) found out about CyberASAP either through a government website or social media, and two each (4%) found out from KTN or from industry contacts.

These routes were broadly similar in Years 1 to 5. The most notable difference between the first five Years and Years 6 to 8 was that 24% of Year 1 to 5 participants who responded to the previous evaluation survey found out about CyberASAP from KTN (n=55), compared to a proportion of 4% in Years 6 to 8 (n=47).

In Years 1 to 5, delivery partner feedback highlighted that communicating the programme and competitions was hindered by the lack of certainty regarding funding for the following year or programme. It is not known until November or December each year, at the earliest, if the programme will be funded for delivery the following April, leaving a short time frame from publishing the call to receiving responses and assessment. It was suggested that if it were possible to market the programme earlier (for example, from June in the preceding year) there could be a greater focus on addressing any regional, diversity, or gender target by engaging with organisations in these areas.

This challenge continued after Year 5 owing to the government's annual planning cycles, although the impact of the problem appears to have shifted: the emphasis from delivery partners was now on having to

[26] See the website here: https://www.plexal.com/our-work/cyberasap-industry-challenges/ (accessed 18/03/2025).

run the competition and assess applications at risk, without funding confirmation from government, rather than a focus on achieving regional, diversity, or gender targets.

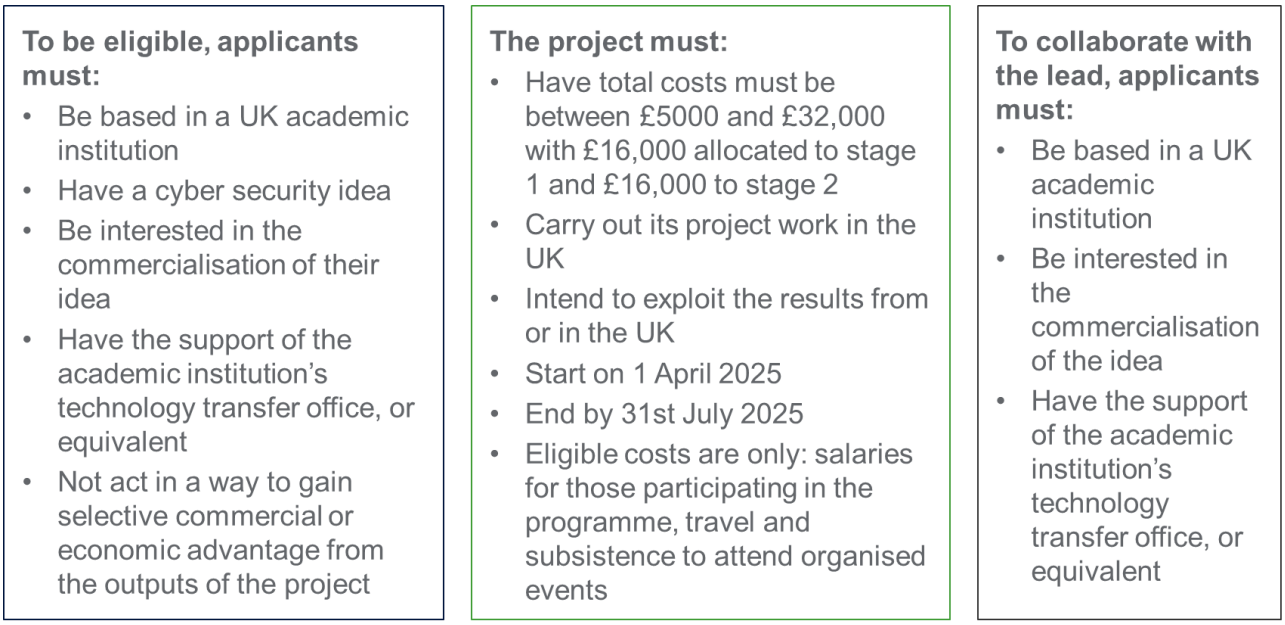
4.3.3 Application process

The following sections provide an overview of the application process and key findings from participants and delivery partners about their experience of the application process.

4.3.3.1 Eligibility

The latest CyberASAP eligibility criteria for applicants are as follows:

Figure 6: CyberASAP eligibility criteria



Source: Eligibility criteria on Innovate UK website - https://iuk-business-connect.org.uk/opportunities/cyber-security-academic-startup-accelerator-programme-year-9-phase-1/ (accessed 05/02/2025)

The criteria have not materially changed since the last evaluation, which covered the first five Years of the programme. The main change during the first five Years was to emphasise the involvement of university technology transfer offices from Year 4 onward. This change was introduced to ensure that university technology transfer officers were involved in the projects from the start of their time on CyberASAP.

Anyone based in a UK-registered academic institution was eligible. Applicants were able to submit more than one application if they had more than one idea. However, only one application from one individual could be selected for funding. Innovate UK offered an online briefing event each Year of the programme. Additional guidance for applicants was available on the government's website[27].

4.3.3.2 Application process

The application process has remained largely unchanged since Year 2. Applicants applied for Phase 1A online, through a standard Innovate UK grant competition. Year 8 applicants could indicate their preferred strand (industry challenge-led or open). However, the assessors chose the strand that best suited the project. Phase 2 was not open for applications from outside the projects selected for Phase 1. Instead, it required progression through a closed competition following successful completion of Phase 1 activities.

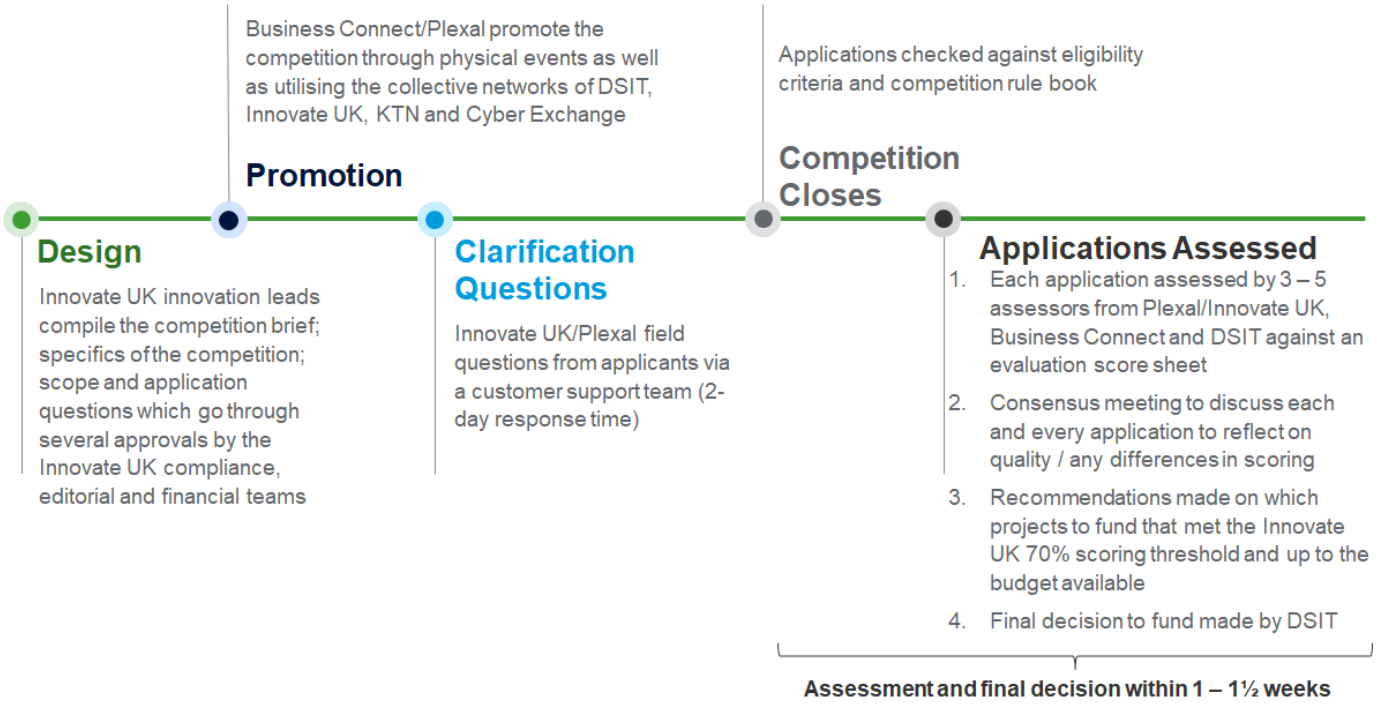
[27] See: https://apply-for-innovation-funding.service.gov.uk/competition/2098/overview/f1e46939-46a6-4388-967b-33a623457419#eligibility (accessed 05/02/2025).

For Year 9, Innovate UK received around 60 completed applications. The growth in the number of applications from a few dozen in the early years likely reflected the growing awareness among academics of CyberASAP. One training provider also suggested that CyberASAP has developed a high level of prestige, noting:

'*CyberASAP has become aspirational, it has prestige to it and people want to be on it*.' – Training provider interview.

Concurrently, this growth introduced new challenges, such as the need to consider how to communicate decisions to the growing number of applicants that were not chosen for funding in Year 9. The following figure summarises the application process.

Figure 7: CyberASAP application process for Phase 1



Source: DSIT (2023) Evaluation of the Cyber Security Academic Startup Accelerator, interviews with RSM

The most common factors that participants who responded to the participant surveys cited for why they applied for CyberASAP were their desire to commercialise their academic research and understand the potential commercial viability of their idea:

'*CyberASAP is a great opportunity to gain commercialization skills and develop a startup from an initial idea*.' – Cohort 8 survey respondent.

In the Year 6 to 8 participant survey, respondents indicated that the application process was straightforward to complete (n=47, 96% of respondents). This high level of satisfaction is unchanged compared to Years 1 to 5.

4.3.4 Support provided

The programme has largely followed a consistent structure and offered similar activities each year. These activities have been well received by all stakeholders, one university TTO noting that '*the [academic] team were buzzing, inspired and excited with the process*'.

Each phase starts with a two-day bootcamp. In line with the increased focus on active involvement of university TTOs, which became more important to the programme following the first five Years, Phases 1A and 2 also include TTO webinars early in each phase. Projects have access to a variety of training sessions prior to mid-programme reviews in Phases 1A and 1B and are required to attend a mix of online and in-person events, including a meet the entrepreneur day in Phase 1B. Phases 1A and 1B each end with a formal assessment of their Value Proposition and Market Validation respectively. Projects progressing to Phase 2 continue to have access to training. They conclude their time on CyberASAP with a demonstration day where they showcase their proof of concept. Industry challenge-led cohort projects are required to attend one additional day of events in Phase 1 and Phase 2 each and have access to industry mentors.

The following table summarises the activities in each phase.

Table 4: CyberASAP support activities by phase

Phase 1A	Phase 1B	Phase 2
Activities: • Bootcamp • TTO webinar • Presentations on e.g. market validation, business models and value propositions • Mid-Programme Review • Assessment Panel • Industry representative mentoring (for industry challenge-led cohort) • Weekly Drop-Ins	Activities: • Bootcamp • Presentations on e.g. PR, pitches, and networking • Mid-Programme Review • Support for applications for Phase 2 • Meet the Entrepreneurs Day • Assessment Panel • Industry representative mentoring (for industry challenge-led cohort) • Weekly Drop-Ins	Activities: • Bootcamp • TTO webinar • 1:1 personal development calls • Industry case study presentations and industry in-person day (for industry challenge-led cohort) • Industry representative mentoring (for industry challenge-led cohort) • Training: Presentation Skills; Investor Pitch Readiness; Sales and Commercialisation; Meet the Investor and Commercialisation Training • Final Pitch Critique and Demo Day Preparation • Demo Day

Source: CyberASAP final reports, logframes, and online information - *https://iuk-business-connect.org.uk/opportunities/cyber-security-academic-startup-accelerator-programme-year-9-phase-1/ (accessed 05/02/2025)*

4.3.4.1 Quality of support provided

In interviews, industry representatives on decision making panels and university TTOs described the support and structure of CyberASAP as unique, as did many academics who participated in the programme. They said it does not, unlike other accelerator programmes, assume that teams have basic knowledge of building and running a business. Instead, it exposes academics to the '*real world*' (training provider) of business.

The role of KTN/Innovate UK Business Connect and the quality of the activities delivered were well received by all the stakeholders involved. They noted that KTN/Innovate UK Business Connect are effective at ensuring that project teams attend all events and activities and that the team provides clear and constructive feedback and advice to projects.

'*I think it's a bit like Dragon's Den. They do lots of reality checks but in a normal language, nothing highfalutin*.' – Training provider interview.

Survey responses from participants in Years 6 to 8 confirm this positive view: 96% of respondents (n=47) found the commercialisation knowledge of KTN staff very helpful (66%) or helpful (30%). The knowledge of Plexal staff received almost equally positive feedback in the participant survey. Similarly, participants who responded (n=47) to the surveys found the knowledge of industry specialists and investors to be very helpful (55%) or helpful (30%). Only two respondents (4%) found their knowledge not helpful.

If a team does not attend as required, KTN/Innovate UK Business Connect quickly reach out to the team to remind them to join. This leads to good attendance and better-quality skills and project ideas. The stage gating, which leads to academic teams getting grant funding iteratively over the course of a year rather than once at the start, provides another incentive for teams to stay engaged with the programme and attend all its activities. It also, according to trainers, helps the programme to '*filter out and support the teams that are really motivated to develop a proof of concept*'. The same trainers also noted that:

'*CyberASAP is good at getting teams to narrow down their ideas or shift their ideas if they're too broad initially*.' – Training provider interview.

One university TTO stressed the value of teams meeting in-person in a central location in London as this enabled networking with each other and with investors that this particular university's team otherwise struggles to meet (the university is located in the north of England). Trainers also noted that in-person activities are preferrable to remote activities but recognised that barriers can exist (e.g., need for longer travel). Some participants echoed this barrier, especially those from universities further away from London.

Surveys asked Year 6 to 8 participants about their satisfaction with the support they received from CyberASAP. With very little variation, participants were either satisfied or very satisfied with the support they received. The only aspects of the programme that received any negative feedback in the survey were the following:

- The selection panels: one respondent each who experienced a selection panel and responded to the question (n=47) were either dissatisfied (2%) or very dissatisfied with the panel (2%).
- The amount of grant funding: one respondent was dissatisfied (n=47, 2%).
- Legal training: one respondent was dissatisfied (n=47, 2%).

This is in line with findings for participants in Years 1 to 5 in the previous evaluation[28].

The same was true for participants' experience of the additional support received from Plexal in Year 8. Respondents who received Plexal support found Plexal mentoring and training either helpful or very helpful. Illustrating this positive feedback, one respondent noted in the survey:

'*Plexal was incredibly helpful in getting us closer to industry through introductions to key stakeholders and workshops delivered by specialised experts for each step of the program*.' – Cohort 8 survey respondent.

The survey asked participants in Years 6 to 8 to explain what aspects of CyberASAP they found worked best. The most common themes that respondents mentioned were the structure of the programme and its focus on building commercialisation knowledge and skills. For instance, in their response, one participant noted:

[28] See DSIT (2023) Evaluation of the Cyber Security Academic Startup Accelerator (available online: https://www.gov.uk/government/publications/evaluation-of-the-cyber-security-academic-startup-accelerator/evaluation-of-the-cyber-security-academic-startup-accelerator#cyberasap-impact-evaluation---performance, accessed 18/03/2025).

'*Strongly systematic training sessions: all these sessions enhancing my skills comprehensively, like marketing validation, project management, sales, presentation, business model, etc. All these sessions make me become a researcher with business thinking rather than just researcher's mind*.' – Cohort 8 survey respondent.

When asked specifically about the extent to which support from university TTOs (or equivalent) was helpful to the participants, 34 of 47 (72%) Year 6 to 8 survey respondents said the support was either helpful to a large extent or to a moderate extent. Six (13%) of respondents said the support was not helpful at all. Illustrating this positive feedback, one survey respondent added:

'*Our TTO is an integral part of our team, and we received continued support in filing our patent application and recruiting/reserving the needed resources to implement our PoC*.' – Cohort 8 survey respondent.

Some specific feedback emerged about the membership of assessment panels. Assessment panel members are primarily volunteers from a relatively small pool of the UK based cybersecurity community. Some have non-technical backgrounds. Some industry representatives suggested that these non-technical panel members may find it harder to understand the technical aspects of projects, which puts a heavier burden on volunteers with technology expertise to explain the projects and their ideas. This, in turn, risks that good ideas are missed or do not progress through the phases but has so far, according to the industry representatives, not led to ostensibly wrong panel decisions. Other representatives, who also provided some of the CyberASAP training, felt that the variety of panel members is positive because it means that teams have access to a variety of views and networks.

Interview feedback on possible gaps on assessment panels or involvement in the programme includes:

- Greater number of representatives from large research heavy UK organisations or businesses (e.g., BAE or Rolls-Royce Holdings). However, it is noted that many of the programme's supporters are from smaller businesses due to their understanding of the early-stage nature of the projects and/or have been on the startup/commercialisation journey themselves. Nevertheless, the programme has had some representatives from larger businesses including BT; BAE Systems; Serco; NCC Group; Siemens; and Crossword Cybersecurity, as well from the investor community relevant to cyber who have been involved in events.[29]
- Chief Information Security Officers to help ensure that projects being assessed by panels have viable business solutions that are relevant to businesses now, not just potentially in future.
- Representatives of the VCSE sector as some ideas are potentially better suited to a not-for-profit business model than a for-profit one (e.g., in childcare or in care for older people).

4.3.4.2 Areas for improvement

Industry representatives noted that early training in business economics could be valuable so that project teams understand the economics of running businesses from the start of the programme. Similarly, some selected project ideas were reported to be little more than initial concepts that may not meet current business needs. Industry representatives suggested that engaging with potential applicants before CyberASAP Phase 1A could help academics conduct initial market research to assess the potential of their idea to solve real, current problems.

[29] Information provided by Innovate UK to RSM UK Consulting LLP (May 2025)

A specific suggestion from training providers for adapting the training was that participants should be required to book one to three events following the networking training to put what they learned into practice. After this, they should report back to Innovate UK and the trainer.

The challenges formulated for the industry challenge-led cohort in Year 8 were broad, representing themes such as cybersecurity supply chains. Industry representatives felt this was too broad to lead to products and suggested that specific business challenges could be more effective in achieving the desired outcomes of CyberASAP.

Assessment panel members, trainers, and participants felt there was scope for improvement in the pitch presentations and panel assessments. A few panel members and trainers suggested that the pitches are inflexible in their design, requiring a structured presentation. This could disadvantage academics from different cultural backgrounds and whose first language is not English. Furthermore, the standard structure and slide format required by teams results in many similar presentations, making it difficult for teams to stand out and tell their individual stories. More flexibility in how teams can present their ideas could allow them to work to their strengths but may require assessment panel members to have more flexible scoring guidance. Similarly, training providers suggested that more time to focus on the visuals and slides that academics use in pitches could further improve their quality. They noted that another day of training for this purpose would be valuable. Academics indicated that they were unaware of the composition of the panel ahead of time, and therefore did not feel well prepared. One academic suggested that it would be helpful if CyberASAP developed a transparent scoring system which also allows teams to submit material before the pitch. In this approach, the final presentation would make up a proportion of the score, with the previously submitted material also contributing to the final score.

TTOs noted that it was important to set clear expectations and rules for investor days, so that ideas presented remained confidential and were not exposed to the risk of potential misappropriation. They did not, however, suggest that any ideas had to their knowledge been acquired in such a way. TTOs stressed that from their university perspective, it was important for teams to engage with them so that the university, which generally owns large parts of the research IP, remain informed of progress. One TTO suggested that TTOs should attend as many in-person events and activities as they can to share insights:

'*There is value in TTOs going to all in-person events. It could be worth more attendance [from them] beyond the workshops to make more and richer connections*.' – University TTO interview.

From the perspective of panel members and trainers, this ownership of IP can discourage otherwise strong projects from progressing after they graduate from CyberASAP. They believe this system risks disincentivising continued efforts to spin out businesses and products. This is a structural issue that is beyond the scope or ability of CyberASAP to address on its own.

Training providers noted that there have been occasional instances where academic teams have not appeared to engage fully in training sessions. For instance, in one case, the academic spent most of the training session on calls. In another case, the academic at the presentation and pitch training was not the person who was going to conduct the actual pitch. Academics who do not fully engage in the training are likely not to get the most out of the training.

4.3.5 Monitoring and reporting

Innovate UK oversees the monitoring process and contracts with monitoring officers who are responsible for checking what projects are delivering and whether this matches expectations. Innovate UK collates information from monitoring officers into monthly monitoring reports to DSIT. The reports provide DSIT with updates on each project's progress and status. The overall achievement of KPIs, a high-level narrative update on progress, risks and mitigations, and financial information is included in monthly logframe reports

from Innovate UK to DSIT. The content and format of logframe reports has stayed largely unchanged since their introduction in Year 5. In Year 8, the logframe reports added reporting on Plexal's KPIs.

Information about KPIs within logframe reports includes updates on the number of teams that progress through the phases of CyberASAP. It also covers:

- Investments raised by CyberASAP projects and companies.
- The number of companies registered by CyberASAP alumni (in total, not just in-year).
- The number of CyberASAP articles published.

As in Years 1 to 5, CyberASAP only has targets for the number of teams progressing through programme phases and the number of articles published per year.

The previous evaluation of Years 1 to 5 made several recommendations for updates to the content of reports. The recommendations were that all KPIs and milestones could have SMART targets and an accompanying narrative about the activities that contribute to milestones and any delays to the achievement of milestones. Furthermore, the evaluation recommended that monthly reporting could include further key outputs and outcomes of the programme, including the number of proof-of-concept demonstrators, new patents and technologies, and market validated value propositions. These recommendations do not appear to have been put into practice but are still relevant because they would allow for in-year assessment of achievement of key outputs.

End-of-year reports from Innovate UK summarise data from monthly logframes and provide detail about the activities delivered along with a running total of companies that have been formed or acquired.

4.3.5.1 Satisfaction with reporting requirements

Evaluation surveys asked participants about their satisfaction with the frequency of reporting, the amount of information required, and the clarity of reporting requirements. Participants in Years 6 to 8 were mostly satisfied or very satisfied with all these requirements, with 87% to 89% of respondents (n=47) across these years selecting these answers.

- 42 (89%) participants responding to the survey were satisfied (47%) or very satisfied (43%) with the frequency of reporting.
- 41 (87%) were satisfied (40%) or very satisfied (47%) with the amount of information required.
- 41 (87%) were satisfied (45%) or very satisfied (43%) with the clarity of reporting requirements[30].

These levels of satisfaction were higher than they were in Years 1 to 5. In Years 1 to 5, satisfaction with these reporting aspects ranged from 70% (n=54) for amount of information to provide to 78% (n=54) for clarity of reporting requirements. This indicates increasing levels of satisfaction with reporting requirements[31].

[30] One respondent each was very dissatisfied with these reporting aspects (2%). 2 (4%) were dissatisfied with the amount of information required and one (2%) was dissatisfied with the clarity of reporting requirements. The remainder were neither satisfied nor dissatisfied or were not sure.
[31] See DSIT (2023) Evaluation of the Cyber Security Academic Startup Accelerator (available online: https://www.gov.uk/government/publications/evaluation-of-the-cyber-security-academic-startup-accelerator/evaluation-of-the-cyber-security-academic-startup-accelerator#cyberasap-impact-evaluation---performance, accessed 18/03/2025).

4.3.6 External factors influencing programme delivery

While the COVID-19 pandemic did not influence delivery of activities for Years 6 to 8 directly, delivery partners noted that projects funded during the pandemic had less exposure to investors and potential customers compared to projects funded outside the pandemic. Innovate UK mentioned this as a key factor driving the need for additional engagement activities with and tracking of alumni.

Government planning cycles, which tend to favour funding for programmes delivered in one financial year, led to Innovate UK operating programme competitions at risk, before knowing whether DCMS/DSIT would fund the following year's activities. This has not led to any reported impacts on actual delivery but was a risk noted in both interviews for the evaluation of Years 1 to 5 of CyberASAP and this evaluation.

Another effect of one-year funding cycles is that support for projects after they graduate finishes, bar alumni engagement. One training provider suggested that there would be value in offering mentorship for two years after graduation in recognition of the fact that commercialisation can take time. However, they acknowledged that finding mentors who can commit for such a long period may be challenging. Another trainer felt that the one-year timeframe does not work equally well for all projects. Some projects have levels of technical complexity that make it unlikely that they can lead to a Proof of Concept within one year, especially given academics' other ongoing commitments.

Survey respondents in Years 6 to 8 (n=47) mentioned three external factors affecting the programme for them:

- 17 reported internal university policies (36%).
- 13 reported difficulties recruiting team members (28%)
- nine reported challenges onboarding people into their team (19%).

30 respondents experienced at least one factor affecting the programme (64%). 17 respondents (36%) did not report experiencing any issues that affected their experiences of the delivery of CyberASAP.

It is notable that the proportion of survey respondents in Years 1 to 5 (n=54) who said that internal university policies affected their experience of the programme was 67%[32], compared to 36% in Years 6 to 8 (n=47). This suggests that the impact of such policies is diminishing but they remain the most cited external factor.

4.3.7 Learnings

4.3.7.1 What worked well

KTN/Innovate UK Business Connect was consistently praised for their hands-on approach to supporting teams progressing through the programme. This resulted in high levels of reported attendance at events, training, and bootcamps. The quality of support provided and the knowledge of those delivering it received very positive feedback. Interest in CyberASAP appears to have steadily increased, resulting in over 60 applications for the programme in 2025/26.

The design of CyberASAP has been adjusted over time in collaboration between KTN/Innovate UK Business Connect, Innovate UK, and DSIT/DCMS to reflect feedback from participants and other stakeholders. Most recently this included additional activities to engage with alumni after they graduate from the programme and to engage with potential applicants before the programme. These additional activities

[32] See DSIT (2023) Evaluation of the Cyber Security Academic Startup Accelerator (available online: https://www.gov.uk/government/publications/evaluation-of-the-cyber-security-academic-startup-accelerator/evaluation-of-the-cyber-security-academic-startup-accelerator#cyberasap-impact-evaluation---performance, accessed 18/03/2025).

are designed to help alumni continue to develop their projects and to contribute to projects that are most likely to benefit from the programme. Most stakeholders and participants praised the fast-paced delivery of the programme, including the stage-gating approach between each phase. The quality of support received, and the knowledge of KTN/Innovate UK Business Connect and Plexal staff were also very positive aspects of the programme, according to participants who responded to the surveys. For most participants, this contributed to high levels of engagement with the content of CyberASAP.

4.3.7.2 What worked less well

University TTO involvement in the programme has increased over time. There are still apparent issues relating to the role of universities in CyberASAP, including the extent to which IP rights and product or company ownership belong to the participating teams as opposed to universities. Survey responses from participants in Years 6 to 8 indicate that the main issue affecting programme delivery remains internal university policies (17 out of 47, 36%, said this was an issue), which includes IP policies and processes. However, this is a notable improvement compared to Years 1 to 5, when 67% of survey respondents (n=54) cited such policies when asked about issues that affected them. Importantly, it may be beyond the scope of the programme to influence such policies, much less change them.

While the stage-gated and fast-paced design and delivery of the programme received mostly positive feedback, there were specific elements of the programme that did not work for all. A few academics felt that the time and resource required from them was not clear when they applied to CyberASAP, and a few senior academics felt that it demanded too much time in a short period, considering their other teaching and research commitments. Finally, some training providers suggested that more flexibility in the content and format of pitch presentations to assessment panels could better suit different projects than a standard approach.

4.3.7.3 Areas for improvement

Specific suggestions for improvements are as follows.

- Early training in business economics could be valuable so that project teams understand the economics of running businesses from the start of the programme. Some form of engagement with potential applicants before CyberASAP Phase 1A could help academics conduct initial prior market research into the potential for their idea to solve a real, current problem, and provide more insight into the content of CyberASAP. Since 2024, Innovate UK run the CyberASAP Pathfinder[33], which is a short-course introduction to the core elements of CyberASAP and which addresses some of these aspects.
- Flexibility in how teams present their ideas between phases could allow teams to work to their specific strengths.
- Participants should be required to book up to three events following the networking training to put what they learned into practice. After this, they should report back to Innovate UK and the trainer.
- The challenges formulated for the industry challenge-led cohort in Year 8 were broad, representing themes such as cybersecurity supply chains. Specific business challenges could be more effective in achieving the desired outcomes of CyberASAP.
- Assessment panels in between phases could be strengthened by including more technologically knowledgeable people, such as Chief Information Security Officers. Panels could also benefit from the inclusion of more large businesses active in the cybersecurity space.

[33] See: https://iuk-business-connect.org.uk/opportunities/cyberasap-pathfinder-2025/ (accessed 04/03/2025).

5. Impact Evaluation

This section provides an assessment of CyberASAP against its key performance indicators (KPIs), delivery objectives, and Theory of Change (ToC) metrics. The key impact evaluation questions to be addressed using this evidence are:

- To what extent has the programme been effective at enabling the academic sector to commercialise their ideas or speed up this process?
- What are the challenges facing academics upon graduation of the programme? To what extent has the programme been effective at mitigating these? How else might the programme support alumni/graduates?
- Assess the causal mechanism with respect to the culture and behaviour of academics (e.g., entrepreneurial skills, perceptions of commercialisation, intent to commercialise) and their institutions and the challenges they face. Consider whether the programme is working as intended.
- To what extent has the programme been effective in bringing research outputs to the marketplace (e.g., spin-out companies, product licensing, and the development of new products and services)?
- Have there been any additional or unintended benefits of the programme (improved commercial awareness, better inter-university collaboration, improved commercial knowledge of university knowledge exchange teams, private sector investment, patents, licenses, open-source software)?

5.1. Summary of key findings

The evidence available suggests that CyberASAP is delivering its intended intermediate outcomes and is showing progress towards longer-term outcomes in the form of successful trading spin-out companies and their economic impacts. Overall, the evidence of impact is strongest for spin-out formation and attracting investment. Many alumni felt the programme was the key factor in their successful company formation and access to investment, and this is backed up by testimonies from TTOs and investors.

Due to the length of time required to generate economic impacts, evidence for the most recent cohorts (6-8) is weaker than that for Cohorts 1-5. However, the evidence for intermediate outcomes – which are steps in the causal chain towards longer-term impacts as set out in the ToC – is encouraging in the short term for Cohorts 6-8. This includes the effect of the programme on the relevant skills, knowledge, and confidence to turn an idea into a viable product or spin-out a company, and the investor readiness and industry connections required to seek out and attract new investment.

Specifically, we have tested four claims about CyberASAP's effectiveness:

A: CyberASAP contributes to the skills and knowledge needed to turn an idea into a viable product.

We find **moderate to strong evidence of a moderate to strong impact**. We have high confidence that CyberASAP enables researchers to refine their ideas into commercially viable products through CyberASAP's phased approach. There is evidence through interviews, survey data, and case studies that academic teams have developed proofs of concept and carried out market validation, and that in many cases they would not have been able to do this without CyberASAP.

B: CyberASAP contributes to the skills, confidence, and knowledge needed to spin-out a company.

We find **moderate to strong evidence of a moderate to strong impact**. The most impactful component of the support is connecting researchers with investors, mentors, and industry partners, where multiple sources (investors, TTOs, founders) confirm that the investor introductions and the phased training were decisive on spin-out formation.

C: Participating in CyberASAP contributes to researchers attracting new investment from private and/or public sources.

We find **strong evidence of a strong impact.** Although some projects might have succeeded in fundraising regardless, CyberASAP's training, investor intros, and brand recognition often prove critical. Qualitatively, CyberASAP is believed to increase the strike rate for investable projects according to investor feedback. This is backed up by quantitative data on the number of companies that have secured funding relative to spin-outs in general.

D: Participating in CyberASAP contributes to high survival rates of companies spun out of university research.

We find **moderate to strong evidence of a moderate impact.** CyberASAP equips spin-outs with the skills, funding, and industry connections needed to help them survive beyond their initial launch. However, these factors alone do not guarantee their survival. University spin-outs generally have a higher early-years survival rate compared to typical start-ups, and the statistical evidence is not sufficiently strong to attribute any significant improvement directly to CyberASAP.

5.2. Key performance indicators

This section assesses performance against the delivery partner's contracted KPIs based on data submitted in logframes to DSIT. It also considers the extent to which this demonstrates CyberASAP's success in achieving its aims.

5.2.1 Assessment of KPIs

CyberASAP has the following KPIs:

- Teams progressing through programme phases.
- Running total investment attracted by CyberASAP projects/companies.
- CyberASAP Alumni Companies registered.
- CyberASAP articles published[34].

From Cohort 5 (2021) onward, two of the KPIs have targets (i.e., teams progressing through the programme; and CyberASAP articles published on the KTN website). The other two KPIs do not have targets (i.e., the total investment attracted by CyberASAP projects outside of CyberASAP funding and the number of companies formed). Progress on the KPIs is reported to DSIT through monthly logframes and annual end of year reports. These KPIs represent some ToC outputs (e.g., applications/cohorts/projects) and intermediate outcomes (increased new cyber security start-ups/spinouts, short-term investment). Most ToC outputs are not monitored or reported monthly, only on a yearly basis. Participant satisfaction with

[34] This refers to online articles about CyberASAP and the projects that progress through the programme, including their ideas and products.

monitoring and reporting requirements was high, suggesting limited additional reporting requirements are unlikely to be perceived as overwhelming.

5.2.2 Performance against KPIs

The table below summarises performance against the four CyberASAP KPIs.

Table 5: Performance against KPIs

Indicator / Target	Performance							
	2017 (Cohort 1)	2018 (Cohort 2)	2019 (Cohort 3)	2020 (Cohort 4)	2021 (Cohort 5)	2022 (Cohort 6)	2023 (Cohort 7)	2024 (Cohort 8)
Teams progressing through programme phases	Target: N/A, Actual: 12	Target: N/A, Actual: 26	Target: N/A, Actual: 26	Target: N/A, Actual: 28	Target: 20, Actual 21	Target: 20, Actual: 28	Target: 28, Actual: 27	Target: 30, Actual: 30
Running total investment attracted by CyberASAP projects / companies (cumulative, £m)	N/A	N/A	Target: N/A, Actual: over 3.2	Target: N/A, Actual: over 7.5	Target: N/A, Actual: 17.7	Target: N/A, Actual: 19	Target: N/A, Actual: 32.3[35]	Target: N/A, Actual: 41
CyberASAP Alumni Companies registered (running total)	Target: N/A, Actual: 9	Target: N/A, Actual: 9	Target: N/A, Actual: 14	Target: N/A, Actual: 20	Target: N/A, Actual: 22	Target: N/A, Actual: 27	Target: N/A Actual: 33	Target: N/A, Actual: 34
CyberASAP articles published	N/A	N/A	N/A	N/A	Target: 12, Actual: 33	Target: 12, Actual: 23	Target: 9, Actual: 7	Target: 11, Actual: 9

Sources: evaluation of Cohorts 1-5 programme logframes, Year 6 end of programme report and KTN data shared with RSM UK Consulting LLP. The source for Cohort 8 is the Year 8, February 2025 Logframe. This year is ongoing at the time of writing the report and the figures in this table are therefore preliminary.

5.2.3 Assessment of KPI performance

The available evidence suggests that CyberASAP has mostly met its KPIs, where targets exist. The exception is Cohort 7, where the target for projects progressing through the phases was missed by one project and the target for articles published was missed by two articles. Year 8 is ongoing and the performance against KPIs for that year is therefore not final.

[35] CyberASAP Snapshot Impact Stats September 2024. At the end of the financial year 2023/24, according to the Year 7, March 2024 Logframe, the total stood at £23m.

There has been a steady increase in the amount of external investment attracted by CyberASAP companies and in the number of companies registered by CyberASAP alumni. This demonstrates success against some of the programme's aims in the CyberASAP ToC, in particular the following intermediate outcomes and long-term outcomes:

- Increased new cyber security start-ups and spin-outs.
- Enhanced business viability and short-term investment.
- Wider commercialisation of academic research and ideas.

5.3. Performance against the Theory of Change

This section uses evidence from multiple sources to assess how effectively CyberASAP is achieving its intended outcomes and impacts. These include:

- **Programme monitoring data:** logframe reports, Innovate UK Innovate UK impact reports (including KPI data on company registrations, investment raised, etc.).
- **Surveys:** two online surveys, designed and implemented by RSM for this evaluation, targeting Cohorts 1–5 and Cohorts 6–8 to gather primary data on commercialisation progress (e.g., spin-outs, IP licensing, new products/services), any additional grants received, and perceived improvements in commercial skills.
- **Interviews**: conducted by RSM with stakeholders (e.g., DSIT, Innovate UK, TTOs, investors) to understand the programme's broader context and potential barriers or enablers.
- **Case studies:** projects from Cohorts 6–8, selected and develop by RSM to illustrate specific outcomes (e.g., new spin-outs, successful fundraising, regional economic benefits).
- **Published data:** Beauhurst, Companies House, ONS (especially for local/regional analysis of spin-outs).

Where available the following has also been incorporated:

- **Budget and spend data:** past financial data from DSIT records or MoU documents for each cohort (1–7) to illustrate cost trends.
- **KPIs:** already listed in section 5.1 (e.g., teams progressing through phases, total investment attracted).
- **Alumni tracking:** where Innovate UK or DSIT holds historical data on spin-outs, new products, or funding raised by prior cohorts.

At this interim reporting stage, the evidence has been used to give a provisional view of CyberASAP's performance, which can be refined for the final report as additional data become available.

This evidence has been used to show the contribution of the programme to each stage of the ToC: activities, outputs, outcomes, and impacts.

5.3.1 Activities and outputs

The main activities and outputs conducted over Years 1 to 8 based on KTN and Innovate UK annual reports are outlined in the following table.

Table 6: Activities and outputs

Year	Activities	Outputs
Years 1-8	• Selection panels and application assessments. • Bootcamps and webinars. • Concept demonstrators / showcase events. • Events such as: Meet the Entrepreneurs Day, Information Security Europe Show. • Training such as: presentation skills, sales and commercialisation, investor readiness, and meet the investor.	• 305 applications, over 170 projects. • 99 Demonstrator events. • 34 companies formed. • Over £40 million in post-programme funding to pursue commercialisation routes across Years 1-8, and include CAPSLOCK, Cavero Quantum, Fact360, KETS Quantum, Lupovis, and Mindgard.

The table above is a summary of available information. A more detailed breakdown of activities delivered in each year and the corresponding outputs achieved can be found in Appendix E. This information demonstrates that CyberASAP is delivering on its intended objectives for activities and outputs.

5.3.2 Intermediate outcomes

The outcome metrics identified in the ToC are distributed between shorter-term intermediate outcomes and long-term outcomes. At this stage evidence of intermediate outcomes – such as gaining in knowledge and confidence, spinning out a company, and trialling products and services – is more prevalent than evidence of long-term outcomes. Performance against each of the intermediate outcome measures is discussed below:

5.3.2.1 Increased number of new cyber security start-ups/spin-outs (company registrations)

Innovate UK monitoring data indicates:

- 34 new companies have been formed over Years 1-7.
- No companies have been formed from current cohort (Year 8).

The running average over Years 1-5 was 5.8 companies per year. However, company formation is a medium-to-long term outcome of the programme, and it is expected that the number of company registrations will increase further from the Year 6-8 cohorts. The survey data, which is more recent than the available monitoring data, suggests that more companies have been set up by participants from Cohorts 6-8; a total of eight among the 33 survey respondents.

The survey also provides early evidence of progress towards company formation among the Cohort 6-8 participants, using the skills gained from the programme. After completion of CyberASAP 75% of participants in Cohorts 6-8 (n=33) developed a proof of concept, with all respondents developing a Value Proposition and 97% completing market validation of their product.

Table 7: Outcomes of participation in CyberASAP (Cohorts 6-8)

	A Value Proposition	Market Validation	Proof of Concept
Yes	32	31	24
No	0	0	5
Not applicable	0	1	2

In addition, several industry mentors and investors panel members described how the programme's sales training and external mentoring helped teams better align their technical ideas with market needs.

5.3.2.2 Enhanced business viability and short-term investment

Of the 33 respondents to the Cohort 6-8 survey, eight respondents suggested they have registered a business. However, only half of these respondents reported that the continued operation of their business was an outcome resulting from participation in CyberASAP. Furthermore, three of the eight respondents that had registered a business feel that it is more likely to survive its early years of operation because of participating in CyberASAP. Therefore, from these cohorts, there is limited self-reported evidence of enhanced business viability and the interview data did not provide strong evidence of such enhancement.

There are not strong conclusions from the most recent cohorts as university spin-outs tend to have low early-stage failure rates compared to conventional start-ups: they benefit from the support of their parent institution and are typically not spun-out without some consideration of their viability. Therefore, it is difficult for CyberASAP to have made a discernible impact on survival in the first few years.

Nine (39%, n=23) respondents from Cohorts 1-5 have either spun out or registered a company. Of these nine respondents, seven (78%, n=9) respondents have businesses that are continuing to operate, and six of these (67%, n=9) felt their business was going to survive its early years of operation. This indicates that self-reported evidence of business viability may strengthen over time following programme completion.

36% of participants who responded to the survey from Cohorts 6-8 (n=33) reported they trialled a new viable product or service because of CyberASAP. Among those respondents in Cohort 1-5, 65% (n=23) reported they have trialled a new product or service. This is likely due to the longer timeframe between programme completion and response, which has allowed this outcome to be realised.

The survey of Cohorts 6-8 found limited evidence of participants securing investment for their products or services beyond CyberASAP. Only 6% of participants (n=33) reported receiving investment, with no clear indication that securing the investment was directly attributable to their participation in the programme. Interviews did not clearly link this investment directly to CyberASAP participation.

Survey respondents also suggest levels of investment increase over the longer term. 30% (n=23) of Cohort 1-5 respondents suggest they have received investment for their product or service, with three of these reporting they have received over £500,000 in investment. Of those who have received investment, they reported that, on average, 90% of this funding could be attributed to CyberASAP participation.

5.3.2.3 Self-reported changes in business knowledge/skills

Participants in Cohorts 6-8 identified business knowledge and skills as the programme's most important impacts. The most frequently cited benefits included improvements in entrepreneurial skills (52%, n=33) and a better understanding of business setup processes (40%). Additionally, participants reported increased confidence in their business skills (55%) This aligns with the most common reasons for wishing to

participate in CyberASAP, with 72% (n=33) reporting they participated to develop their entrepreneurial skills and 62% reporting they participated to develop their knowledge of the business set-up process.

One interviewee stated, '*I never encountered market validation or pitching techniques in my academic work; CyberASAP opened my eyes to these crucial skills*'. Other interviewees emphasised that the training and mentoring components boosted their commercial confidence. This increased substantially for Cohorts 1–5, with all respondents (n=23) reporting an improvement in their commercial awareness. This highlights CyberASAP's strong impact, particularly over the longer term, in enhancing participants' business skills and knowledge, equipping them with the expertise needed to navigate commercialisation more effectively.

5.3.2.4 Increased confidence, aspiration, and resilience to form and run businesses

Among CyberASAP participants from Cohorts 6-8, 55% (n=33) of survey respondents reported that increased confidence in their ability to form and run a business was one of the most important impacts of their participation. In contrast, fewer participants identified the programme's impact on resilience in managing business challenges (12%) or its role in increasing their aspiration to start and run a business (18%) as their most important impacts. However, when considering broader outcomes, 52% (n=33) of respondents stated that CyberASAP increased their aspirations to start and run a business, and 36% reported an improvement in their resilience in managing business challenges, even if these were not ranked among the most important impacts. However, multiple interviewees described a '*mind shift'* among academics toward viewing commercialisation as a viable and even attractive option. Even if they did not believe that involvement in commercialisation of Intellectual Property (IP) would be part of their academic career going forward, they were able to think more about how market-relevant or user-focused the outputs of their research could be.

5.3.2.5 More funding leveraged (public, grants, university)

Funding leveraged was identified as the programme's most substantial realised outcome by respondents to the survey. 65% of participants (n=33) from Cohorts 6-8 who responded to the survey reported securing additional funding, either fully or partially due to their participation in CyberASAP. Of these, 36% of participants indicated they had received funding in the form of a government grant for their service or product since completing CyberASAP. Similarly, 61% (n=23) of Cohort 1-5 respondents reported securing further funding however a lower proportion indicated they have received government grants since completing CyberASAP (26%).

One interviewee stated that the '*CyberASAP grant acts as a lever*', opening doors to discussions with potential investors and university decision-makers, leading to access to additional funding sources. Those who received grant funding in Cohorts 6-8 (n=12) reported varying grant sizes, as set out in Table 8. The median amount received was £75-100k.

Table 8: Amount of funding through government grants received by CyberASAP Cohort 6-8 participants after completion

Amount of funding	Number of participants
Up to £24,999.99	1
£25,000 - £49,999.99	0
£50,000 - £74,999.99	3
£75,000 - £99,999.99	3
£100,000 and above	4
Prefer not to say	1

The distribution of grant amounts was slightly different for Cohort 1-5 respondents, with 50% (n=6) of those receiving grants suggesting they have received over £100,000 of government grants since completing CyberASAP. However, the levels of in-kind investment reported increased with 94% (n=33) of respondents from Cohorts 6–8 reporting they had not received in-kind investment for their products or services. In contrast, this figure drops to 70% (n=23) among respondents from Cohorts 1–5, who have been out of the programme for a longer period. In cases where in-kind support was provided, it typically came in the form of loans, expertise/advice from other companies, and additional resources, with a median investment of £40,000.

This suggests as time passes after completing CyberASAP participants may have greater opportunities to secure in-kind investment and highlights the potential longer-term impacts of the programme.

5.3.2.6 Entry into other incubator/accelerator programmes

Before CyberASAP, only 9% (n=33) of participants in Cohorts 6-8 had participated in other programmes aimed at supporting the commercialisation of research into cyber security. After participation in CyberASAP, 24% of participants (n=33) entered other related programmes. The programmes they entered included ICURe, university accelerators, external accelerators, and cyber bootcamps. One participant explained '*CyberASAP gave me the credibility to join other accelerator programmes and attend alumni networking events that opened additional funding pathways*.' Several interviewees echoed this sentiment.

5.3.2.7 Increased industry input to help shape and validate market relevant technologies, products, and services from academia

Several interviewees noted that industry experts—whether through sales training workshops or direct mentoring—provided critical feedback that helped academic teams align their innovations with market needs. While the Year 8 challenge-led approach aimed to incorporate explicit industry-defined problem statements, the interview data do not firmly confirm that this led to systematically '*better'* or more extensive industry input compared to the open cohorts. For instance, one mentor noted, '*having real-world problems from industry is very useful, but we didn't see a direct, across-the-board advantage just because it was challenge-led.'* The challenge-led format did help some teams identify a clearer product-market alignment, but further evidence would be needed to demonstrate improved outcomes specifically for that cohort compared to earlier or open-cohort participants. Intermediate outcomes such as improved networking skills and enhanced commercial confidence received strong qualitative support, whereas direct links to increased investment remain less evidenced.

5.3.3 Longer-term outcomes

The longer-term outcomes identified in the Theory of Change occur after company start-up and initial trialling of products or services (usually after five to ten years). They include:

- Greater early years survival rates
- Wider commercialisation of academic research and ideas
- Greater acceleration, incubation, and growth in the UK cyber sector
- Spillover impacts.

These are unlikely to materialise during participation in CyberASAP or immediately after graduation, as they require additional time and effort using the skills and resources gained to commercialise IP and grow successful companies. The evidence of performance against these is detailed below; this is mainly qualitative and due to the timing of each cohort, the evidence from Cohorts 6-8 is limited.

5.3.3.1 Greater early years survival rates

While only three companies from Cohort 6 have formally spun out to date (with no companies yet from Cohorts 7 and 8), several industry stakeholders and university TTOs indicated that projects are actively trading and attracting follow-on funding.

According to our survey, six businesses, representing 35% of those from Cohorts 1–8 (n=56), have ceased trading to date. While this figure may seem significant, it is important to consider it in the context of broader tech start-up survival rates. Research indicates that approximately 57% of start-up dissolve within two years across the time period of CyberASAP[36]. In comparison, CyberASAP-supported businesses demonstrate a relatively high survival rate, suggesting that the programme may provide participants with crucial commercialisation skills, market insights, and networking opportunities that contribute to their resilience. However, this finding should be interpreted with caution due to the small survey sample size, which may not fully represent the broader population of CyberASAP participants.

5.3.3.2 Wider commercialisation of academic research and ideas - drawing technical expertise and capabilities out of universities

Several academic researchers and TTOs repeatedly stressed that CyberASAP has transformed academic mindsets regarding commercialisation. For example, evidence from Cohorts 6-8 respondents to the survey suggests CyberASAP has enhanced academics' ability to commercialise cyber security research. Before participation, participants self-reported an average capability score of four out of ten. Following the programme, this increased substantially to an average of eight out of ten. Notably, the minimum reported score rose from one out of ten before participation to five out of ten afterward. This suggests that participants from universities increased their ability to commercialise research substantially from participating in the programme.

Table 9: Difference in self-reported commercialisation capabilities pre- and post- CyberASAP participation (N=33)

	Capability before participation	Capability after participation
Mean	4.27	8.18
Minimum	1	5
Maximum	10	10

There is also some evidence from respondents from both Cohorts 1-5 and Cohorts 6-8 of research being commercialised through licencing models, trademarks, and patents. Specifically of Cohort 6-8 respondents (n=33), the following are reported because of participation in CyberASAP:

- 18% have developed a licensing model.
- 3% have secured a trademark.
- 6% have secured a patent.

[36] PwC analysis finds failure rates amongst startups at lowest level in a decade, despite record company formations

The levels of commercialisation have increased slightly for Cohorts 1-5 (n=23):

- 30% have developed a licencing model.
- 4% have secured a trademark.
- 13% have secured a patent.

5.3.3.3 Greater acceleration, incubation, and growth in the UK cyber sector

Industry investors and programme mentors cited examples of companies accelerated through CyberASAP – such as Mindgard and several spin-outs that have secured subsequent investment rounds – demonstrating a measurable impact on the cyber sector's growth.

Though the projects selected for case studies have not yet gone on to receive subsequent investment post-participation, they consistently noted that their experience has increased their confidence in being able to do so moving forward. Additionally, several project teams interviewed for case studies have experienced significant evolution in their products because of involvement, including production of a proof of concept and achieving legal status as a company.

5.3.3.4 Spillover impact: UK universities more agile in supporting academic research commercialisation – in cyber and beyond

Multiple TTOs and university administrators said that CyberASAP prompted internal reviews of intellectual property and commercialisation policies and procedures at their institutions. However, they did not indicate that the reviews have led to specific changes at this time.

5.3.3.5 Spillover impact: Contribution to the local ecosystem

Interview data suggest spin-outs may contribute to local economies by creating jobs and attracting follow-on investments. However, these observations are tentative and largely self-reported.

5.3.3.6 Industry experiences fewer barriers through challenges identified

Several panel members – including industry investors and programme mentors – provided examples demonstrating how CyberASAP lowered the traditional barriers between academia and industry. One panellist stated, '*CyberASAP's targeted training and mentoring bridged the cultural and knowledge gaps that typically keep academic innovations isolated from market realities*.' Specifically, CyberASAP facilitated dialogues between a university's researchers and industry partners, leading to accelerated prototype development and commercial trials. Another case from a different university Year 8 challenge-led cohort demonstrated how mentorship from industry veterans helped an academic team secure commercial partnerships more swiftly, clearly illustrating the programme's role in fostering industry engagement.

5.3.3.7 Productive companies with turnover/revenue

To date the evidence indicates:

- Several CyberASAP alumni are generating revenue and have secured follow-on funding, for example Mindgard (Cohort 6 participant) are reportedly the number one AI model security company in the world and have raised over £9m[37].

[37] Mindgard has raised approximately £9 million in funding across multiple rounds. The latest round in December 2024 secured $8 million (TechCrunch), while a previous round raised $3.8 million in 2023 (Crunchbase). Using the average exchange rate at the time (1 USD ≈ 0.7911 GBP), this equates to a total of approximately £9.34 million.

- 89% (n=9) of those respondents to the Cohort 1-5 survey who had registered a company believe their company is now more productive due to, or partly because of, participating in CyberASAP.
- 44% (n=9) of respondents from Cohorts 1–5 who registered a company have experienced an increase in turnover since participating in CyberASAP. This suggests that the programme has played a role in supporting productive businesses by enhancing participants' commercial awareness.

However, it is not unusual for start-up companies to operate at a loss for several years before their product offering and market penetration has developed to the extent that they can trade profitably (the "cash burn" phase of the start-up life cycle, when it is consuming its available cash from initial investments).

5.3.3.8 UK academic space recognised as a leading source of cyber solutions amongst industry leaders/industry stakeholders

Feedback from industry stakeholders and TTOs suggested CyberASAP is increasingly viewed as a flagship initiative that boosts the credibility of UK academic cyber research among investors and industry leaders. For example, one investor commented '*CyberASAP has significantly enhanced the reputation of academic cyber innovations in the investment community*'.

5.3.3.9 New technologies, products and services adopted in the UK and internationally

One industry advisor reported that CyberASAP spin-outs secured contracts with international partners, while another project reached licensing deals with multiple educational institutions. (Note: these examples represent tentative evidence from the limited sample of companies that are sufficiently mature to be exploring these opportunities and should be interpreted with caution).

5.3.3.10 Greater diversity and inclusivity across the cyber sector

Several academic researchers and industry mentors commented on the need for improved gender balance and inclusivity. While the welcoming nature of the programme was highlighted by some female participants, others suggested that increased female representation would have made them feel more confident during their time on the programme. Evidence from the surveys suggests:

- There has been an increase in female representation within the programme - Cohorts 1-5 data show only 13% of participants (n=23) were female, this increased to 34% (n=33) for Cohorts 6-8.
- there is also a slight increase in ethnic minority representation between Cohorts 1-5 and Cohorts 6-8, rising from 30% (n=23) to 38% (n=33).

This indicates CyberASAP is contributing to greater diversity and inclusion in the sector by increasing participation among both female and ethnic minority entrepreneurs. However, while this progress is positive, ongoing efforts are needed to further enhance representation and ensure equitable access to opportunities across all demographics.

5.4. Contribution analysis with process tracing

The extent to which CyberASAP meaningfully contributed to spinning out companies, raising investment, and boosting commercialisation skills was tested using **contribution analysis** and **process tracing** to assess the strength of evidence to support or refute four claims about the effectiveness of the programme.

Contribution analysis assesses the available evidence for each claim against that for alternative explanations for the observed outputs and outcomes. The following table outlines the contribution claims and alternative hypotheses.

Table 10: Contribution claims

Claim	Alternative Hypothesis
CyberASAP contributes to the skills and knowledge needed to turn an idea into a viable product.	The researchers turned their idea into a viable product irrespective of skills and knowledge developed through CyberASAP
CyberASAP contributes to the skills, confidence and knowledge needed to spin-out a company.	Cyber security academics have commercialised their research due to factors independent of CyberASAP (e.g., private companies, or other initiatives).
Participating in CyberASAP contributes to researchers attracting new investment from private and/or public sources.	Researchers attracted investment due to reasons independent of CyberASAP.
Participating in CyberASAP contributes to high survival rates of companies that spun out of university research.	Spun out companies either don't survive or survive because of other factors than CyberASAP.

The following classification of levels of contribution were used:

- **Strong contribution** - indicates that CyberASAP has achieved substantial results with few or no other contributing factors.
- **Some contribution** - indicates that CyberASAP has achieved some, but no substantial results with evidence that other contribution factors are at play.
- **Negligible contribution** - indicates that CyberASAP has not or not yet achieved any or only very limited results or that the results are effects of other contributing factors.

Evidence was gathered from stakeholder interviews, surveys, case studies, and programme monitoring data to assess CyberASAP's role in supporting viable product development, spin-out formation, investment attraction, and company survival.

There are four process tracing tests[38] that can be used to assess the qualitative strength of the evidence and the extent to which the specific support provided by CyberASAP contributes to the various outcomes/impacts achieved. These are:

- **"Straw in the wind" tests** – these are used to describe evidence that can be indicative but is neither sufficient nor necessary for the theory, therefore weak.

[38] Ricks, J. I. and Liu, A. H. (2018) 'Process-Tracing Research Designs: A Practical Guide', *PS: Political Science & Politics*, 51(4), pp. 842–846. Cambridge University Press.

- **"Hoop" tests** – failing this test disqualifies the hypothesis (it has failed to "pass through the hoop"), but success does not guarantee that the hypothesis is true; it is necessary but not sufficient.
- **"Smoking gun" tests** – passing such a test lends strong support to the theory, but failure is not necessarily disqualifying. It is sufficient evidence to prove the theory, but not necessary.
- **"Double decisive" tests** – if the evidence passes the test, it strongly supports the theory, and failure counts strongly against the theory – they are both necessary and sufficient.

Collectively, these identify whether the causal mechanisms described in the contribution claims are sufficient and/or necessary to explain the outcomes.

The four contribution claims are evaluated in the following tables with CyberASAP's contribution strength, and the robustness of the evidence.

5.4.1 Claim A: CyberASAP contributes to the skills and knowledge needed to turn an idea into a viable product.

CyberASAP provides researchers with commercialisation training, market validation support, and proof-of-concept funding, equipping them with the knowledge and confidence to develop market-ready products.

Table 11: Claim A – Assessment

Contribution statement	Evidence	Strength of CyberASAP's contribution to the result	Strength of evidence
CyberASAP enables researchers to refine their ideas into commercially viable products.	Multiple academics and TTOs report that CyberASAP's structured curriculum, mentoring, and market validation exercises significantly improved their ability to develop products. One interviewee stated that '*the look, feel, and functionality of our product improved by about 40% due to CyberASAP*.' Others highlighted that without CyberASAP their projects would have remained as internal university research tools rather than market-facing products.	**Strong** – Many participants indicated they would not have developed a viable product without CyberASAP.	**Strong** – interviews, survey data, and case studies consistently confirm improved prototypes.
CyberASAP enhances researchers' commercialisation skills.	Investors highlighted increased commercial awareness and ability to pitch to stakeholders. One investor noted that CyberASAP significantly improved product presentations over time, stating that in early years	**Moderate to Strong** – Some researchers would have gained commercialisation skills elsewhere, but CyberASAP accelerated the process.	**Strong -** Investors, TTOs, and academics align on the programme's pitch training benefits.

Contribution statement	Evidence	Strength of CyberASAP's contribution to the result	Strength of evidence
	'*presentations were weak, but now they are clear, compelling, and investor-ready*.'		
CyberASAP's cohort model fosters peer learning and networking.	The structured peer-learning approach enables researchers to gain insights from others facing similar commercialisation challenges. An industry mentor noted '*CyberASAP pulls people together, and that cohort advantage is a multiplier*.'	**Strong** – The peer-learning and networking elements are consistently praised as critical enablers of learning, knowledge exchange, and motivation.	**Moderate** – Some qualitative evidence supports this, but outcomes are harder to measure.

The evidence aligns with a "smoking gun" scenario: for many participants, CyberASAP was a key catalyst that accelerated or directly enabled the development of viable products. While a few participants noted they might have eventually developed prototypes through alternate grants (e.g. ICURe) or internal funds, interviews show many would not have done so – or would have stalled – without CyberASAP.

5.4.2 Claim B: CyberASAP contributes to the skills, confidence, and knowledge needed to spin-out a company.

CyberASAP provides participants with structured guidance on business models, IP strategy, and investor readiness, enabling them to transition from research projects to spin-out companies.

Table 12: Claim B – Assessment

Contribution statement	Evidence and other contributing factors	Strength of CyberASAP's contribution to the result	Strength of evidence
CyberASAP builds confidence among researchers to pursue spin-outs.	Many academics reported that without CyberASAP, they would not have considered spinning out. A university TTO stated '*colleagues now see a pathway to commercialisation that wasn't obvious before*.'	**Strong** – participants repeatedly cite the programme as key to building spin-out confidence.	**Moderate to Strong** – some TTO or other university support might have existed, but CyberASAP is widely cited as the essential factor.
CyberASAP supports spin-out formation by connecting researchers with investors, mentors, and industry partners.	Case studies highlight that spin-outs like Mindgard and R1 Collective emerged due to CyberASAP, receiving early-stage support and guidance. An investor noted '*CyberASAP is outperforming traditional*	**Strong** – the introduction to investors and the methodical training on spin-out formation appear decisive.	**Strong** – many cross-verified sources (investors, TTO, founders) confirm the direct effect.

Contribution statement	Evidence and other contributing factors	Strength of CyberASAP's contribution to the result	Strength of evidence
	investment routes in identifying promising startups.'		
Some projects choose technology licensing as their primary route-to-market rather than spinning out, as licensing can better suit technologies requiring substantial upfront investment or industry-specific capabilities.	While spin-outs are a primary focus, some participants license their technology instead. One academic noted '*we're selling under license rather than spinning out, but CyberASAP helped refine our product for that model*.' This alternative does not detract from the programme's role in building commercialisation skills; in fact, for some academics it may be the case that the knowledge that CyberASAP provides on the nature of spin-outs gives them the perspective they need to realise that licensing is the superior commercialisation option for them.	**Moderate** – CyberASAP supports multiple commercialisation pathways, not just spin-outs.	**Moderate** – Cases exist where spin-out was not the best option.

The evidence suggests a "smoking gun" effect for spin-outs: while not necessary, CyberASAP is sufficiently influential that its presence strongly correlates with the decision and ability to spin-out (or license). The interviews and data strongly refute the idea that participants would have commercialised entirely on their own.

5.4.3 Claim C: Participating in CyberASAP contributes to researchers attracting new investment from private and/or public sources.

CyberASAP provides early-stage funding, enhances investor readiness, and facilitates industry connections.

Table 13: Claim C – Assessment

Contribution statement	Evidence and other contributing factors	Strength of CyberASAP's contribution to the result	Strength of evidence
CyberASAP increases researchers' ability to secure investment.	Over £40m of follow-on funding has been secured by CyberASAP alumni, with some startups receiving multiple rounds of investment. A venture capitalist stated '*CyberASAP at least doubles the strike rate for investable projects compared to typical university spin-outs.'*	**Strong** – Direct links between CyberASAP participation and funding success are evident.	**Strong** – Supported by quantitative funding data and investor feedback.

Contribution statement	Evidence and other contributing factors	Strength of CyberASAP's contribution to the result	Strength of evidence
CyberASAP's challenge-led cohort design improves market alignment.	Investors note that CyberASAP's challenge-led approach improves the likelihood of securing funding. However, one mentor cautioned '*many CyberASAP projects still don't meet clear market needs.'*	**Moderate to Strong** – While thematic challenges help, not all ideas are automatically investor-worthy.	**Moderate** – feedback from mentors, but limited data so far since the challenge-led approach has only been piloted in Cohort 8 so far.
Programme credibility and brand opens doors	Participants say that the '*badge'* of being a CyberASAP graduate encourages investor interest. One TTO stated '*we had far better responses from VCs once we mentioned we came through CyberASAP.'*	**Strong** — the reputational boost often leads to additional investor meetings.	**Moderate** —qualitative evidence from interviews rather than a large sample-based measure.

The evidence suggests a "smoking gun" effect: although some projects might have succeeded in fundraising regardless, CyberASAP's training, investor intros, and brand recognition often prove critical. The presence of the programme strongly correlates with improved investment outcomes.

5.4.4 Claim D: Participating in CyberASAP contributes to high survival rates of companies spun out of university research.

CyberASAP equips spin-outs with the skills, funding, and industry connections needed to survive beyond their initial launch.

Table 14: Claim D – Assessment

Contribution Statement	Evidence and Other Contributing Factors	Strength of CyberASAP's Contribution to the Result	Strength of Evidence
CyberASAP contributes to long-term survival of spin-outs.	Several CyberASAP alumni companies, such as Mindgard and R1 Collective, remain active, securing additional funding and commercial contracts. A TTO representative noted '*without CyberASAP's early support, the company may not have survived*.'	**Moderate to Strong** – the programme clearly supports early traction, but survival also depends on external factors (market, leadership, cash).	Moderate – we have multiple case examples, but not broad, long-term data across all cohorts.
The alumni network and post-programme support help sustain spin-outs.	Some founders mention bridging finance or advanced alumni sessions as 'lifesavers.' Others suggest they still lack stable resources or ongoing mentorship once the programme ends.	**Moderate** – post programme support is valuable, but broader factors influence survival.	Moderate – alumni references are positive but partial and self-reported.

CyberASAP supports company survival but is not always a decisive factor— it is not necessary for company survival, and it is not sufficient to guarantee company survival on its own, though the evidence suggests that it contributes, particularly in later cohorts. The evidence suggests "Straw in the Wind" category – it points in the direction that CyberASAP has been helpful, however it is not possible to confirm it made a difference to business survival for any specific cases relative to what would have occurred in its absence.

5.5. Bayesian updating

We have employed "Bayesian updating" to extend the analysis above to provide transparent, quantified statements of how confident we are that CyberASAP caused the observed outcomes. To achieve this, we have converted the assessments of evidence for each of claims A to D set out above into probability estimates, taking conservative values from ranges set out in guidance for impact evaluation.[39]. The higher the **strength of evidence**, the more confident we are that CyberASAP is having an impact. Conversely, the higher the **strength of CyberASAP's contribution to the result**, the lower our estimate that the results observed among participants are "false positives" attributable to other causes.

Table 15: Quantitative assessment of strength of evidence

Assessment of strength of evidence	Probability of CyberASAP impact	Probability of "false positive"
Moderate	60%	40%
Moderate to strong	67.5%	32.5%
Strong	75%	25%

The full calculations and results are provided in Appendix G; a summary is provided below.

Claims A and B are assessed solely using the qualitative evidence set out in the previous section. Secondary quantitative evidence is available for the likelihood of academics developing commercialisable IP and spinning out companies; however, this is not comparable with the CyberASAP cohorts because of selection bias. The academics that join CyberASAP are different to most academics in that they have commercialisable IP and/or a strong interest in spinning out a company.

Based on the qualitative evidence, **we are 94% confident of Claim A**: "CyberASAP contributes to the skills and knowledge needed to turn an idea into a viable product". The strongest evidence is "CyberASAP enables researchers to refine their ideas into commercially viable products", which has a Bayes factor of 3.

We are 92% confident of Claim B: "CyberASAP contributes to the skills, confidence, and knowledge needed to spin-out a company". The strongest evidence is "CyberASAP supports spin-out formation by connecting researchers with investors, mentors, and industry partners", which has a Bayes factor of 3.

Claims C and D are supported by external quantitative evidence as well as the qualitative evidence laid out in the previous section. For Claim C (attracting investment), analyses from Beauhurst and sector studies show that, in early-stage academic spinouts, securing external investment is challenging, with only around 10–15% attracting significant private or public funding in the early years. By contrast, our central estimate of CyberASAP spin-outs that have attracted significant external investment is 59%. For Claim D, external data suggest that survival rates for academic spinouts can be relatively high (around 60–70% over three years)[40]

[39] Befani, B., & Stedman-Bryce, G. (2016). Process Tracing and Bayesian Updating for impact evaluation. *Evaluation*, *23*(1), 42-60. https://doi.org/10.1177/1356389016654584 (Original work published 2017)
[40] UK Office for National Statistics (ons.gov.uk), HESA HE-BCI Survey (hesa.ac.uk), and various UK Small Business Statistics reports

due to strong intellectual property and university backing. Out of 29 spin-outs in cohorts 1-5 for which we have been given management information, 3 have been dissolved (10.3%) and 2 are reported as dormant (6.9%), giving a survival rate of 83-90% depending on whether dormant companies are included.

We are 98% confident of Claim C: "Participating in CyberASAP contributes to researchers attracting new investment from private and/or public sources". The strongest evidence is the observed rate of investment relative to other spin-outs, which has a Bayes factor of 3.9.

We are only 78% confident of Claim D: "Participating in CyberASAP contributes to high survival rates of companies spun out of university research". None of the evidence is particularly significant, but the qualitative evidence that "CyberASAP contributes to long-term survival of spin-outs" is the most convincing, with a Bayes factor of 1.85.

5.6. Effectiveness of CyberASAP

The section answers the following 'effectiveness' evaluation questions:

5.6.1 To what extent has the programme been effective at enabling the academic sector to commercialise their ideas or speed up this process?

There is strong evidence that CyberASAP has contributed significantly to increasing the skills and knowledge needed to turn an idea into a viable product, particularly in enabling researchers to refine their ideas. Survey respondents reported a substantial increased capability to commercialise their research following participation in the programme as:

- Prior to participating in the programme 3% (n= 1 of 33 respondents) ranked their capability to commercialise research between eight and ten (with ten meaning "very strong").
- Following participation 73% (n= 24 of 33 respondents) ranked their capability to commercialise research between eight and ten [41].

5.6.2 What are the challenges facing academics upon graduation of the programme? To what extent has the programme been effective at mitigating these? How else might the programme support alumni/graduates?

The challenges identified by panel members were 'traditional' barriers of knowledge, experience, and confidence affecting contact between academia and industry. The programme has contributed to alleviating these through its development of skills and knowledge required to engage with industry, and the confidence and motivation to apply these.

Participants also identified internal university policies as the most frequent challenge faced when trying to commercialise their research, followed by recruitment difficulties and challenges with onboarding people onto their teams.

5.6.3 Assess the causal mechanism with respect to the culture and behaviour of academics (e.g., entrepreneurial skills, perceptions of commercialisation, intent to commercialise) and their institutions and the challenges they face. Consider whether the programme is working as intended.

There is moderate to strong evidence that CyberASAP has affected the behaviour of academics with respect to their adoption of entrepreneurial culture. The programme has contributed to the skills, confidence, and knowledge needed to spin-out a company. Beyond that, it has affected the propensity to commercialise.

[41] The scale from which this data was taken ranged from zero to ten

Evidence for the causal mechanism for commercialisation comes from the reports of many researchers who attribute their decision to spin-out to the structured CyberASAP support. The specific mechanisms can be due to increased confidence, an explanation of a route to commercialisation that was not previously considered, and the networking and connections to further forms of support and advice which the programme provides to facilitate spin-out formation.

5.6.4 To what extent has the programme been effective in turning research outputs into the marketplace (e.g., spin-out companies, product licensing, and the development of new products and services)?

The programme significantly increases the probability of successful spin-out formation and accelerates the process by providing early-stage commercialisation expertise that many researchers lack. While it is too early to observe significant market impact from Cohorts 6-8, earlier cohorts have spun out companies, licensed technology, and developed products and services. Among 23 alumni in Cohorts 1-5 captured in our survey, seven have developed a licencing model, and 15 have trialled a new viable product or service.

There are also examples of further knowledge and IP generation, through registration of patents and provision of outputs in open-source format. In the Cohort 1-5 survey, three respondents had secured a patent for a product or service, one had secured a trademark, and seven have developed open-source software.

5.6.5 Have there been any additional or unintended benefits of the programme (improved commercial awareness, better inter-university collaboration, improved commercial knowledge of university knowledge exchange teams, private sector investment, patents, licenses, open-source software)?

There have been several additional benefits of the programme beyond those captured in its key performance indicators. As set out in the sections above, the programme has led to improved commercial awareness, which has in turn affected how alumni think about their research through a market lens. The survey evidence has also reported private sector investment, and dissemination of IP through patents and open-source software.

A key additional benefit has been through licensing. The primary route to commercialisation supported by CyberASAP is spin-out company formation; however, IP licensing is an equally valid pathway to market[42] and is more suitable in some instances where working with established companies is preferable (for example, in sectors with high capital costs). Some CyberASAP projects have licensed their technology instead, and 1 specifically reported that the skills learned in the programme helped them to refine their product for that model.

[42] Research into issues around the commercialisation of university Intellectual Property (RSM, 2018, for BEIS) considers spin-outs and IP licensing as the two primary forms of knowledge exchange / commercialisation transaction.

6. Value for Money Evaluation

This section provides an assessment of the economic benefits and value for money CyberASAP has delivered. The key evaluation questions are:

- To what extent has the program used public resources in a way that maximises public value?
- Is this programme the best possible use of public funds to achieve the intended outcomes?[43]
- How could value for money be or have been improved?

This section presents an analysis of programme costs against budgets, and the programme's key monetisable benefits to date (jobs, investment, products/licensing, and economic spillover effects). These will be used to inform a Green Book compliant calculation of return on investment, based on these costs and benefits. However, as the later cohorts are at an early stage, the main sources of evidence for value for money, aside from performance against budgets, are qualitative. We have followed National Audit Office guidance to provide an early assessment of the programme's economy, efficiency, effectiveness, and equity (the "4 'E's" approach) using all the available information.

6.1. Summary of key findings

The overall conclusions from the 4Es assessment are:

- **Economy**: Good. The programme manages budgets effectively, minimises overhead via volunteer mentors, and adapts design (e.g. partial remote delivery) to reduce costs. It has delivered against its targets while underspending for most cohorts.
- **Efficiency**: Good. It aligns phased gating with resource constraints, covers a diverse range of universities, and produces Proofs of Concept (PoCs) and pitches with relatively modest staff/time inputs—though advanced deep-tech solutions need more tailored mentor input. The programme has delivered its outputs at lower-than-budgeted cost per academic team; this is partly due to reduced costs from online delivery. Underspends are recycled to future delivery via DSIT but could be directed to additional support within cohorts.
- **Effectiveness**: Good–Excellent. Repeated spin-outs (30+), multi-million investment rounds, and TTO confirmation of '*accelerated commercial readiness'* point to strong outcome achievement. There are some drop-outs between phases meaning that not all participants generate spin-outs; however, the '*stage gating'*, which tests the quality of the value proposition and market validation before teams can proceed to subsequent phases, is intended to raise the survival rate of eventual spin-outs.
- **Equity**: Good. The programme's shift to hybrid sessions broadens regional access. Although female and minority representation remains below the overall working-age population, there has been a significant improvement over time and compares favourably with other tech programmes (many of which report single-digit percentage rates for female participation) and therefore could be rated as 'good'[44]. Female representation among CyberASAP participants has risen from 13% (Cohorts 1-5) to 34% (Cohorts 6-8). For comparison, the female share of the UK working-age population is around 51%[45] and the proportion of female postgraduates in STEM around 31%[46].

[43] The guidance in the Invitation to Tender suggested that this question should look beyond assessing whether the benefits are greater than the costs, and that it would be helpful to measure the cost per output generated.
[44] Over one million women now in STEM occupations but still account for 29% of STEM workforce
[45] Women In STEM Statistics: Progress and Challenges - Stem Women
[46] Women in STEM Statistics - Stem Women

The evidence for specific evaluation questions (EQs) is outlined below.

6.1.1 To what extent has the program used public resources in a way that maximises public value?

The 4Es assessment suggests that CyberASAP exhibits strong "Good" overall value for money, with particularly strong results in spin-out formation and follow-on investment, while continuing to refine its approach for deeper deep-tech support and improved diversity. It has met its targets on participation and progress while staying within budget.

The rate of spin-out creation is a highlight of CyberASAP, along with the reported evidence that the programme accelerated the timelines for academics who thought they might have commercialised even without CyberASAP support.

By its nature, CyberASAP has low deadweight - it is stimulating economic activity which is unlikely to have arisen from other sources. This is because it is aimed at commercialising novel IP, involving academic researchers who may not have considered launching a spin-out without the support (with evidence of this from surveys of participants). As a result, while economic impacts might take longer to arise than would be the case for support aimed at established businesses, the resulting products and services can be more innovative, less likely to displace or crowd out activity from other businesses, and in the long term could be able to trade internationally.

6.1.2 Is this programme the best possible use of public funds to achieve the intended outcomes?

Targets for team participation and progress have been achieved without using the full allocated budget. The amount of private investment levered into CyberASAP spin-outs is already greater than the total allocated budget.

Table 16: Summary of CyberASAP budget and expenditure in nominal and real terms

Cost measure	Amount (£)	Notes
Allocated budget (nominal)	14,050,073	Sum of budgets from 2018/19–2024-25
Nominal actual spend	9,793,238	8,565,469 (through 2023/24) + 1,227,769 (2024/25 actual so far)
Adjusted spend (2024/25 prices)	11,197,940	9,970,171 (through 2023/24) + 1,227,769 (same in real terms for 2024/25)

Source: DSIT financial records and RSM analysis (2025). Note - figures assume the 2024/25 year is still in progress and final spend may rise

To assess how much spin-out investment has been generated for each pound of public funds, we can compare the full £40 million with the cost figures above or first apply an attribution factor of 70%[47] (derived from survey & case study evidence) to account for deadweight and other influences (meaning 70% of the observed investment is credibly attributed to CyberASAP, and only 30% "deadweight" would have occurred anyway).

After adjusting each cohort's incremental investment to 2024/25 prices, the cumulative real terms total at Cohort 8 is approximately £43.91 million. Nominally, this equates to around £40 million.

[47] Both case-study and survey responses, projects reported a wide range of how much of their external investment they attributed to CyberASAP—anywhere from 30 to 100%. In between, others reported 60%, 70%, or 80%. As the programme was sometimes the decisive factor, but in other cases just one of several enablers 70% was chosen as a balanced, realistic estimate of CyberASAP's contribution overall. This reflects the typical midpoint in the data and ensures the programme's impact on securing external investment is not overstated or understated.

Table 17: Cumulative investment attracted by CyberASAP spinouts in nominal and real terms

Investment measure	Amount (£)	Notes
Nominal cumulative investment	40,000,000	Tally of spin-out investment in nominal terms (unadjusted)
Real-terms cumulative investment	43,907,000	Equivalent 2024/25 value (incremental deflator approach; final total at Cohort 8)

Source: CyberASAP spinout survey data and RSM analysis (2025)

In real terms, the project expenditure to date of £11.20 million has given rise to £43.91 million of investment. The ratio of £43.91 million / £11.20million ≈ 3.92. That is, to date, £3.92 of spin-out investment has been generated for every £1 of actual expenditure in 2024/25 prices.

Attribution at 70%. Acknowledging that some spin-out investment would have happened without CyberASAP, we apply a 70% attribution factor due to deadweight. In this case, £29.18m of investment is estimated to be due to CyberASAP. Under these assumptions, every £1 of programme expenditure in real terms has generated ~£2.74 of net additional spin-out investment across Cohorts 1–8.

6.1.3 How could value for money be or have been improved?

Overall VfM could be improved by management of the underspend by either: a) increasing the numbers accepted into Phase 1, recognising that approx. 50% will drop out between Phase 1A and Phase 2; or b) reducing the budget for Phase 2. Alternatively, the underspend could be proactively directed to additional targeted support for those academic teams which do proceed to later phases, based on their challenges, weaknesses, and needs.

The 4Es assessment identified some areas where improvements would be necessary to achieve a “good” standard:

- **Economy**: The programme manages budgets effectively, minimises overhead via volunteer mentors, and adapts its design (e.g., partial remote delivery) to reduce costs. Some procurement and governance improvements could further enhance efficiency in cost allocation—namely: systematically tracking in-kind mentor contributions, formalising TTO involvement in cost control, and strengthening procurement protocols for external services. See section 6.5.1.
- **Efficiency**: The phased gating approach aligns with resource constraints, engages a diverse range of universities, and delivers PoCs and investor pitches with modest staff/time inputs. However, improvements in quality of outputs such as demos and final pitches—particularly in deep-tech projects requiring more tailored mentor expertise—could enhance efficiency further. See section 6.5.2.
- **Effectiveness:** CyberASAP has enabled over multiple spinouts, with multiple projects securing multi-million-pound investment rounds. TTOs confirm that participants accelerate commercial readiness, significantly shortening the time from research concept to spin-out. However, more tailored support for advanced deep-tech teams would strengthen the programme’s impact. See section 6.5.3.
- **Equity**: The shift to hybrid sessions has broadened regional access, and representation of female and minority academics has increased—though still below parity. Additional targeted outreach and inclusive participation measures could further improve diversity. See section 6.5.4.

6.2. Programme costs against budgets

This section examines CyberASAP's actual spend against its MoU budget. Understanding how the programme's funds have been allocated and utilised provides a foundation for assessing cost-effectiveness and Value for Money. Programme expenditure data from DSIT's financial spreadsheets, MoUs, invoices, and logframes have been analysed to show:

- **Budget vs. actual spend**: the original budget allocations from MoUs vs. actual spend for Years 1–8 from invoices, to detect under/overspend and cost variations over time.
- **Breakdown by delivery partners**: high-level distribution of funds (e.g., grants to participants, management costs, programme administration).
- **Per-participant costs**: where feasible, calculating total direct programme costs divided by the number of participants in each cohort, as part of cost-effectiveness analysis.

This section outlines the budget[48] and actual spend per year. All values exclude VAT.

Table 18: Overall MoU Budget vs. Actual Spend by Year (as at February'25)

Year	MoU Budget	Spend	Variance	Likely cause(s) of underspend
2017/18	N/A	N/A	N/A	No data available from the pilot period.
2018/19	£2,144,523	£1,515,993	£628,530 (29%)	A lower-than-forecast number of teams advanced to Phase 2, so maximum PoC grants were not fully used. Some teams spent less than their Phase 1 allocations (e.g. lower subcontractor costs). Delivery partner efficiencies (fewer in-person events).
2019/20	£2,655,040	£1,577,907	£1,077,133 (41%)	The transition from Phase 1B to Phase 2 saw several teams not pass selection or withdraw. A partial switch to online sessions in early 2020 reduced event costs. Some teams did not claim their full allocated budgets.
2020/21	£1,967,600	£1,561,735	£405,865 (21%)	Remote delivery during the Covid 19 period meant that many in-person elements were replaced by virtual working, lowering travel and workshop costs. Several teams paused or scaled back research, lowering costs. Fewer Phase 2 participants fully used their PoC funding.
2021/22	£1,383,032	£1,061,506	£321,526 (23%)	The remote/hybrid approach continued this year, lowering costs. Some teams did not use their maximum possible Phase 2 allocations.
2022/23	£1,495,500	£1,326,295	£169,205 (11%)	From the year's data, not all who started Phase 1 progressed. Phase 1B and Phase 2 were undersubscribed. There was an ongoing reliance on virtual events (with lower overheads).

[48] This amount is the funds allocated to CyberASAP through each Year 1-8 MoUs

Year	MoU Budget	Spend	Variance	Likely cause(s) of underspend
2023/24	£2,117,388	£1,522,033	£595,355(28 %)	Fewer teams advanced beyond Phase 1A and Phase 1B, resulting in lower Phase 2 participation than budgeted. Cost savings were achieved through digital marketing, group mentoring, and the use of in-kind mentors.
2024/25	£2,286,990	£1,227,769 (to date)	N/A	Year still in progress, therefore full costs not yet incurred
Total	**£14,050,073**	**£9,793,238 (to date)**	**£4,256,834 (30%)**	Best available figures from known financial data, but likely incomplete and missing full 2024/25 figures

Source: CyberASAP programme data and RSM analysis (2025)

From 2018/19 to 2023/24, the total allocated budget – or total amount allocated to the programme via each Cohort'ss MoU's - was £14,050,073. Actual spend over that same period was £9,793,238 which is less than the total amount DSIT budgeted.[49] This arises from a need to ensure sufficient funds to cover the expenditure of the potential number of all academic teams that might complete the programme and historic DCMS practice where the MoU budget was typically 10% higher than the expected invoice total.

6.2.1 Costs per participating academic team

Each year, CyberASAP estimates the total amount it might spend per academic team in each phase (Phase 1A, 1B, or combined Phase 1; and Phase 2). This estimated budget includes:

- Grant funding each team could potentially claim (e.g., to cover researchers' time, travel, PoC development).
- A notional share of delivery partner costs (KTN/Innovate UK Business Connect, Plexal, Innovate UK admin & monitoring) allocated across the teams in that phase.

Hence, the "budgeted cost per team" is the maximum that might be spent if each team fully utilised its phase grant and if delivery partner expenditure matched their estimate. The "actual cost per team" is what was ultimately spent, averaged across the teams that participated in that phase. The following tables compare budgeted vs actual cost per academic team from 2018/19 to 2024/25, subdivided by the main phases of CyberASAP support. In the first two years (2018/19 and 2019/20), phases 1A and 1B were invoiced separately, whereas from 2019/20 onwards, the programme simplified its invoicing into a single "Phase 1" plus "Phase 2." The tables reflect this, with a combined Phase 1 cost used from 2019/20 onwards.

[49] It should be noted the DSIT budget for CyberASAP is the maximum available and not what InnovateUK/programme participants are expected to spend. Therefore, the difference between this figure and the actual spend is not considered 'underspend' by DSIT.

Table 19: Budgeted vs Actual CyberASAP Cost per Academic Team by Phase — 2018/19

Phase	Budgeted Cost/Team	Actual Cost/Team	Variance
Phase 1A	£12,860.35	£12,860	£0.10 (0%)
Phase 1B	£22,701	£17,596	£5,105 (22%)
Phase 2	£106,064	£89,061	£17,003 (16%)

Source: CyberASAP programme management data and RSM analysis (2025)

Table 20: Budgeted vs actual CyberASAP cost per academic team by phase — 2019/20

Phase	Budgeted Cost/Team	Actual Cost/Team	Variance
Phase 1	£63,510	£45,968	£17,542 (28%)
Phase 2	£106,526	£50,658	£55,868 (52%)

Source: CyberASAP programme management data and RSM analysis (2025)

Table 21: Budgeted vs actual CyberASAP cost per academic team by phase — 2020/21

Phase	Budgeted Cost/Team	Actual Cost/Team	Variance
Phase 1	£57,400	£44,256	£13,144 (23%)
Phase 2	£76,292	£48,330	£27,963 (37%)

Source: CyberASAP programme management data and RSM analysis (2025)

Table 22: Budgeted vs actual CyberASAP cost per academic team by phase — 2021/22

Phase	Budgeted Cost/Team	Actual Cost/Team	Variance
Phase 1	£51,685	£46,931	£4,754 (9%)
Phase 2	£76,281	£55,371	£20,911 (27%)

Source: CyberASAP programme management data and RSM analysis (2025)

Table 23: Budgeted vs actual CyberASAP cost per academic team by phase — 2022/23

Phase	Budgeted Cost/Team	Actual Cost/Team	Variance
Phase 1	£50,962	£33,769	£17,193 (34%)
Phase 2	£81,230	£38,892	£42,338 (52%)

Source: CyberASAP programme management data and RSM analysis (2025)

Table 24: Budgeted vs actual CyberASAP cost per academic team by phase — 2023/24

Phase	Budgeted Cost/Team	Actual Cost/Team	Variance
Phase 1	£55,425	£42,332	£13,093 (24%)
Phase 2	£86,133	£55,209	£30,924 (36%)

Source: CyberASAP programme management data and RSM analysis (2025)

Table 25: Budgeted vs actual CyberASAP cost per academic team by phase — 2024/25

Phase	Budgeted Cost/Team	Actual Cost/Team	Variance
Phase 1	£61,914.06	£41,981[50]	£19,933 (32%)
Phase 2	£83,753	N/A[51]	N/A

Source: CyberASAP programme management data and RSM analysis (2025)

Phase 2 typically shows a larger underspend than Phase 1 per team; this is always the case in absolute terms, and in most cases in percentage terms as well. There are several reasons for this:

1. The maximum available funding per team is generally larger in Phase 2 than in Phase 1 (to cover Proof of Concept development) - when fewer teams progress or claim less than expected, the absolute difference (in £) can be more significant than in Phase 1.
2. Dropouts after Phase 1 - even if Phase 1 had 20 participants, not all proceed to Phase 2 due to the selection panel's decisions or participants' own choices. This creates unclaimed Phase 2 budgets. To a lesser extent, this applies to dropouts between Phase 1a and 1b, which inflate the overall cost per team for Phase 1.
3. Partial claims - Some teams do progress to Phase 2 but do not require the full anticipated Proof of Concept development costs (e.g., because of cheaper subcontractors or staff changes). If the difference is large, the underspend is bigger because Phase 2's potential grant is higher.

6.2.1.1 Sample Breakdown of Budget vs. Actual (2022/23 and 2023/24)

The following tables for 2022/23 and 2023/24 provide a more granular split of budget and spend across cost factors (grant contributions, Innovate UK admin, KTN/Plexal delivery). This level of line-by-line expenditure detail is not available for earlier years.

- The "cost per team" figures above are worked out based on the total spending over the number of teams in that phase.
- The breakdown tables below show which specific cost factors (e.g. grants, admin, delivery) contributed to that total spend.

[50] This figure is complete from information shared, as of February 2025, there may be more costs incurred from Phase 1, beyond this period but these are outside the scope of this analysis.
[51] These costs are not included, as our analysis only covers expenditure incurred up to the end of February 2025. Any Phase 2 costs expected to arise in March 2025 fall outside the current reporting period and are therefore not yet accounted for.

- In both years, underspend across all lines contributes to the overall difference from the budget. The most significant factor is the amount of DCMS/DSIT grant, which contributes to budget variance if fewer teams progress to Phase 2).

Table 26: Breakdown of budget vs spend by cost factor — CyberASAP 2022/23

Cost Factor	Budget	Spend	Variance	Explanation (where available)
Innovate UK admin & monitoring	£91,500	£84,401	£7,099 (8%)	Some project management tasks cost less than anticipated.
DCMS/DSIT grant contribution	£1,132,000	£969,894	£162,106 (14%)	Lower than expected number of academic teams, and the grants that did proceed were less expensive than budgeted.
KTN Delivery	£272,000	£272,000	£0 (0%)	

Source: CyberASAP financial reporting data and RSM analysis (2025)

Table 27: Breakdown of Budget vs Spend by Cost Factor — CyberASAP 2023/24

Cost Factor	Budget	Spend	Variance	Explanation (where available)
Innovate UK admin & monitoring	£117,000	£94,161	£22,839 (20%)	Fewer overheads and staff costs than expected.
DCMS/DSIT grant contribution	£1,484,000	£1,015,272	£468,728 (32%)	Some teams did not require the full grant budget.
KTN Delivery	£380,478	£266,592	£113,886 (-30%)	Core training elements moved online, giving rise to resource savings.
Innovate UK procurement costs for Challenge-led Delivery Partner	£50,000	£41.667	£8,333 (17%)	N/A
Challenge-led Delivery Partner (Plexal) costs	£85,910	£104,342	-£18,432 (+21%)	

Source: CyberASAP financial reporting data and RSM analysis (2025)

Observations and conclusions on programme costs:

1. Underspend has occurred annually at a relatively constant level; years 2-7 were all in the range 21-29% except Year 3 (41%) and Year 6 (11%). Reasons for the underspend over the years may have included:
    - Changing costs: Lower overhead from remote/hybrid working,
    - Cohort composition: Fewer teams than expected, and certain cohorts (due to Covid and remote models adapted subsequently) requiring less travel/events,
    - DSIT continues to budget for the maximum possible usage of the scheme to avoid under-budgeting
2. Caution is advised when comparing 2018/19 to subsequent years. Early on, Phase 1 was split into 1A/1B invoices, whereas from 2019/20 onward, a simplified single “Phase 1” approach was used.

3. Because the current FY is ongoing, it is not yet possible to gauge final spend or underspend. However, the pattern of partial underspend may continue if actual claims fall short of budget.

Overall, from in most years a significant proportion of teams drop out or do not pass selection before Phase 2. Each unclaimed Phase 2 slot removes a large chunk of potential spend. Thus, underspend is closely tied to actual participant progression:

- Fewer participants at Phase 2 → fewer PoC grants → bigger Phase 2 underspend.
- Similarly, if some teams in Phase1 do not invoice their full grant, that also contributes to unspent Phase 1 budgets, albeit typically smaller amounts than Phase 2

In the subsequent sections on benefits and Return on Investment, we will use these actual spend figures to contextualise the economic value derived from CyberASAP. Our cost estimates capture direct programme costs (grants, Innovate UK admin, KTN/Plexal delivery). Indirect DSIT staff costs are excluded because these are not ring-fenced within the programme budget; similarly, overhead time from policy teams is not accounted for.

6.3. Programme benefits

In line with our evaluation plan, we have compiled and categorised the monetisable benefits from CyberASAP into four main areas:

1. Employment gains (jobs created or safeguarded)
2. Private investment (venture/seed funding, angel, etc)
3. New products and licensing (any associated value or revenue streams)
4. Spillover effects (e.g. local multipliers, broader collaborations, intangible impacts)

The data is drawn from:

- CyberASAP end of year reports
- Alumni tracking updates (Years 1-6 and partial Year 7)
- Participant surveys (Years 1-5, 6-8)
- Business databases: Beauhurst and RSM Tracker
- Innovate UK data on spin-outs (formation date, current status, funding, employment).

We use aggregated figures so as not to disclose any spin-out–level details that Innovate UK provided in confidence.

6.3.1 Employment gains

CyberASAP's monitoring system does not systematically require participants to report the exact number of jobs each year, we have only partial data, mostly from participants surveys of Cohorts 1-5 and 6-8, alumni tracking updates, Innovate UK figures, and Beauhurst data on selected registered companies. Data from Innovate UK indicates that participating spin-outs collectively employ approximately 102 people, reflecting known headcounts confirmed via founder discussions or verified public sources. To supplement the management information, we searched Beauhurst data for all companies formed through CyberASAP. Employee count data was available for 27 companies, with the majority (59%) having fewer than five

employees. This aligns with the monitoring data, which indicates that most spinouts are still in early stages of development and have relatively small workforces.

Table 28: Employee Counts of CyberASAP Spin-outs (Beauhurst Data, n=27)

Employee count	Number of spinouts	Proportion
<5 employees	16	60%
5-9 employees	5	20%
10-24 employees	5	20%

Source: Beauhurst (2024 snapshot)

The participant survey responses and TTO updates confirm that the majority of CyberASAP spin-outs have 1–3 employees. These include small spin-outs in early stages, some of which have not yet disclosed full details. Among Cohorts 1-5, 11 participants responded to our follow-up survey on employment impacts. They reported 23 new employees in their companies that they considered attributable to CyberASAP. This self-reported figure does not include participants who either did not respond or who did not form spin-outs.

6.3.2 Private investment

CyberASAP regularly tracks investment – venture, angel, or seed – secured by projects after (and sometimes during) the programme, as one of the programme KPIs. The end-of-year reports show steady growth in cumulative external funding across Years 1-6. Updated information from Innovate UK suggests that spin-outs—across various cohorts—have attracted approximately £40 million in external funding to date. This figure excludes certain undisclosed acquisition sums for spin-outs that have exited. Selected companies where information on investment is available through a combination of project reports, stakeholder interviews and our survey are set out below in Table 29.

Table 29: Illustrative external investment (Years 1–6)

Spin-out / project	Approx. investment	Attribution to CyberASAP (survey / Alumni)
KETS Quantum	£10m+	Partial: e.g. 60–70% (source: alumni highlight)
Lupovis	£2.08m	*'Major factor'* says stakeholder, citing early pitch training
Mindgard	£3m	'*CyberASAP was a big influence*' (survey)
Cavero Quantum	£2.19m	'*Partial'* – progressed from partial ICURe involvement
CityDefend	£2m total (approx.)	(Licensed in 2023; the spin-out dissolved)

Source: CyberASAP follow-up participant survey, Alumni highlight reports

The RSM survey of all CyberASAP participants found 16% (n=56) of respondents suggested that they had received further private investment for their product or service. The survey used a banded question to gain information on investments, rather than exact amounts. The table below shows the distribution of private investment received by CyberASAP spinouts/projects.

Table 30: Investment amounts received by CyberASAP participants from the survey (Cohorts 1-8)

Amount of investment	Number of respondents	Proportion
£0	1	11%
£0-£24,999.99	0	0%
£25,000-£49,999.99	1	11%
£50,000-£99,999.99	0	0%
£100,000-£249,999.99	2	22%
£250,000-£499,999.99	1	11%
£500,000 or more	4	44%

Source: CyberASAP Follow-Up Participant Survey – Cohort 1-5 (n=9)

These respondents also reported that, on average, 90% of this funding could be attributed to their participation in CyberASAP. If this ratio were to be applied to the ~£40m recorded investment, it would suggest that £36m could be attributed to CyberASAP.

The survey of the most recent participants (Cohorts 6-8) shows that only 6% reported receiving investment so far, typically between £50k–£500k. However, over 60% of participants from Cohorts 6–8 said they plan to seek additional funding in the future.

6.3.3 New products and licensing

One of CyberASAP's goals is to help participants translate academic research into viable products or services. Where relevant, some projects opt for licensing deals—an equally valid commercialisation route. However, cohort-by-cohort data on the precise number of products or licences is only partially recorded.

The following table summarises outcomes for each CyberASAP cohort (Years 1–6). It shows how many new companies were formed, which spin-outs or projects were acquired or licensed, and when teams released their work as open source. Together, these details illustrate the variety of commercialisation pathways—spin-outs, acquisitions, licensing, and open-source development—that participants have pursued over the programme's different cohorts.

Table 31: Commercialisation outcomes by CyberASAP Cohort (Years 1–6)

Cohort (Year)	Companies formed	Acquisitions	Licensing	Open Source	Illustrative examples
Year 1 (2017)	5 • Awen • Cambridge Authentication • GraphicsFuzz • KETS Quantum • ZORB	2 • GraphicsFuzz (by Google) • Awen (by Sapphire, then by NTT Data)	1 • Cambridge Authentication	–	Awen, Cambridge Authentication, GraphicsFuzz, KETS Quantum, ZORB

Cohort (Year)	Companies formed	Acquisitions	Licensing	Open Source	Illustrative examples
Year 2 (2018/19)	7 • CAPSLOCK • CityDefend • CrypTier • Cydon • Cymond • Raven Science • SEEV	–	2 • AirID • CityDefend	–	CAPSLOCK, CityDefend, SEEV
Year 3 (2019/20)	7 • BLEmap • FACT360 • Onlyn Shield • PhishAR • Seclea • Shoji • Verifiable Credentials	1 • Verifiable Credentials (by Crossword Cybersecurity)	–	–	FACT360, PhishAR, Shoji, Verifiable Credentials
Year 4 (2020/21)	7 • Cavero Quantum • Cybermind • Lupovis • MemCrypt • Riskocity (MaCRA) • Spyderisk • Surface RF	–	–	1 • Secure Development	Cavero Quantum, Lupovis, MemCrypt, MaCRA
Year 5 (2021/22)	3 • FedCam • OSIRT Limited • Tymlo	–	–	2 • MLighter • CyberSignature	OSIRT, MLighter
Year 6 (2022/23)	3 • Lasting Asset • Mindgard • True Deploy	–	–	1 • IoTrim	Mindgard, IoTrim

Sources: DSIT documents: snapshot impact stats sept 2024, Alumni and project highlights

For Years 7–8, data are still emerging. Early indicators suggest at least four new products from Year 7 nearing an advanced prototype stage. One (p-CTI) has lined up an industry partner for a pilot licence, though the deal is not yet final.

For Year 8, it is too early to track final product or licensing outcomes, as most teams only recently completed Phase 2 or are still finalising their demonstrators.

There is some evidence of sales in the Cohort 1-5 survey. Four companies (out of eight respondents) reported an increase in turnover. Among them, 25% saw an increase of £0–£49,999, 50% reported an increase of £50,000–£99,999, and the remaining 25% experienced a rise of £100,000–£249,999. However, only one company directly attributed this growth to their participation in CyberASAP.

Below are selected examples (some from earlier cohorts) that demonstrate how CyberASAP teams typically move from research to a licensable or saleable product:

- CityDefend: IP licensed to multinational Baseel Ltd in 2023 (the original spin-out dissolved, but the product continues under licence).
- Cambridge Authentication, AirID, MLighter: Also licensed or made open-source.
- GraphicsFuzz: Acquired by Google (Year 1 highlight).
- OSIRT (University of Hertfordshire): Now a commercially operating forensic tool.

The precise licensing revenues vary widely (and are often commercially sensitive).

Among the most recent cohorts (6-8), the participant surveys show that about 6% of respondents have licensed technology since finishing CyberASAP.

6.3.4 Spillover effects

"Spillover effects", where benefits from CyberASAP arise in the wider economy, can arise through adoption of new products and services, supply chain relationships, and through movement of personnel. The latter effect is hard to measure, but significant; people who learn new skills through membership of a CyberASAP academic team, or through subsequently joining a start-up, can spread these skills throughout the economy as they move to new jobs and share their learning. Evidence from interviews with TTOs, participant surveys, and alumni events highlight the following:

- **Review of university policies and culture:** several TTO interviewees reported that their institutions have reviewed internal IP and commercialisation guidelines as an indirect consequence of CyberASAP projects. While these reviews have not led to formal policy changes, TTOs noted '*heightened awareness'* of how academic IP can be commercialised in a more agile way. One TTO specifically recounted, describing how a CyberASAP participant's progress led the board to open discussions about making spin-outs more attractive to academic founders. In addition, academics mentioned a '*mindset shift'* among peers who learned that commercial routes need not conflict with research priorities. There was also a realisation these routes can lead to further research and innovation activity, future licensing revenues, stimulation of further R&D investments, and can attract advanced manufacturing or service provision in the UK, thereby enhancing the overall innovation ecosystem.
- **Collaboration effects -** multiple participants (Year 6–8 survey) described forging collaborations with academics they met during CyberASAP bootcamps, sometimes in entirely different fields. This cross-pollination of ideas was seen by TTOs as '*a lasting shift*' that would not have occurred without CyberASAP's structured cohort model and alumni events.
- **International competitiveness -** some investors and industry mentors interviewed noted that CyberASAP spinouts, once visible in the marketplace, helped showcase the quality of UK academic research more broadly. One industry panel member cited '*significant interest'* from a multinational firm that, upon discovering a CyberASAP graduate's technology, began exploring partnerships with other university-based cyber labs in the UK. This can indirectly boost the reputation of the UK academic system as a reliable source of innovative cyber solutions.
- **Increased local economic dynamism -** while most direct company formation remains relatively small-scale (1–3 new jobs per spin-out initially), local economies can still benefit when these spin-outs base themselves near campus or within existing regional tech clusters. Survey data highlights that a participant from a Year 7 spin-out collaborated with local SMEs for prototyping and testing, generating '*additional*

subcontractor revenues' in the region. TTOs suggested that once spin-outs scale, these local linkages may grow, supporting supply-chain and talent development within their locality.

- **Diffusion of commercialisation skills back into teaching and research -** several academics from the Year 6–8 survey explained they had begun sharing newly acquired commercial awareness with doctoral students and early-career colleagues—e.g. incorporating market validation exercises into module coursework or final-year projects. One lecturer stated '*we embedded a mini 'value proposition' assignment in the final-year cybersecurity course so that undergrads get a taste of real-world commercial thinking*.' These examples suggest that, even where a spin-out is not formed, the skill-building aspects of CyberASAP may drive lasting improvements in teaching, curricula, and research approaches.

Taken together, these spillover effects point to broader systemic changes, with CyberASAP acting as a catalyst for institutional openness to commercialisation, regional economic linkages, and dissemination of entrepreneurial skills in academia. While it remains challenging to fully quantify the economic value of such intangible benefits, participant surveys and interviews consistently underscore that these second-order impacts are significant in sustaining a more vibrant academic-to-industry pipeline.

6.4. Return on investment assessment

6.4.1 Monetisable benefits against costs

The Green Book recommends a set of methods to assess the costs and benefits of CyberASAP and compare their monetary values. When fully quantified, the monetary benefits can be compared with total programme costs to estimate value for money indicators such as benefit-cost ratios and Return on Investment.

As the information on benefits comes from different cohorts and has been captured at different times throughout the operation of CyberASAP's yearly cohorts, we have had to account for time lags where data are incomplete (e.g., spinouts formed but not yet reporting revenue). We have estimated missing data for CyberASAP companies using average figures, trends from earlier cohorts, and sector benchmarks. To compare CyberASAP's monetisable benefits with its programme costs, we have converted all historical expenditure into real prices (2024/25) terms using GDP deflators. This allows us to present total costs and investments in real terms, and to derive metrics such as cost per job and investment leverage ratios. In parallel, alternative employment scenarios are developed to reflect both conservative (named spinouts with employment known from management information) and maximum (including employment estimates via Beauhurst data) estimates.

6.4.1.1 Real value of costs

Programme costs since 2018/19 have been adjusted to reflect price inflation. The nominal spend of £9,793,238 in prices current at the time is equivalent to £11,197,940 in 2024/25 prices. Details of this calculation are set out in Appendix H. Investment figures are recorded on a cohort-by-cohort basis. These nominal investment values are similarly adjusted to current values. Table 32 presents the disaggregated investment performance. By Cohort 8, the total nominal investment stands at £40 million.

Table 32: Cumulative total investment attracted by CyberASAP projects (nominal and adjusted)

Cohort (year)	Cumulative Nominal (£ million)	Incremental Nominal (from previous cohort)	Deflator (Year) (2024/25 = 100)	Incremental Investment in 2024/25 Prices (£ m)	Cumulative Total in 2024/25 Prices (£ m)
Cohort 1 (2017)	N/A	–	–	N/A	–
Cohort 2 (2018)	N/A	–	–	N/A	–
Cohort 3 (2019)	3.2	3.2	81.1	3.2 x (100 ÷ 80.1) ≈ 3.94	3.94
Cohort 4 (2020)	7.543	7.543 − 3.2 = 4.343	85.5	4.343 x (100 ÷ 85.5) ≈ 5.08	3.94 + 5.08 = 9.02
Cohort 5 (2021)	17.7	17.7 − 7.543 = 10.157	85.0	10.157 x (100 ÷ 85.0) ≈ 11.95	9.02 + 11.95 = 20.97
Cohort 6 (2022)	19.0	19.0 − 17.7 = 1.3	91.0	1.3 x (100 ÷ 91.0) ≈ 1.43	20.97 + 1.43 = 22.40
Cohort 7 (2023)	32.3	32.3 − 19.0 = 13.3	96.3	13.3 x (100 ÷ 96.3) ≈ 13.81	22.40 + 13.81 = 36.21
Cohort 8 (2024)	40.0	40.0 − 32.3 = 7.7	100.0	7.7	36.21 + 7.7 = 43.91

Source: Internal CyberASAP KPI and investment tracking records (DSIT financial spreadsheets and programme reports) adjusted using ONS GDP deflator data

6.4.1.2 Employment estimates and cost per job

We derive two employment scenarios:

- minimum estimate: based on verified spinouts from Innovate UK data totalling 102 employees.
- maximum estimate: using aggregated Beauhurst data reporting 127 employees across 26 companies.
- For our analysis, we apply an attribution factor of 70%[52] to the reasonable estimate, resulting in:
- Attributable Jobs (minimum) = 102 × 0.70 ≈ 71 jobs
- Attributable Jobs (maximum) = 127 × 0.70 ≈ 89 jobs

[52] *This figure is the average of reported values reported in the participant survey where respondents recorded figures within a wide range—from as low as 30% to full (100%) attribution—reflecting that for some projects CyberASAP was seen as the decisive factor in securing funding, while in others it was one of several contributing influences*

Programme cost per job is calculated using three expenditure metrics:

1. Nominal actual spend: £9,793,238
2. Allocated budget: £14,050,073
3. Real spend (2024/25 prices): £11,197,940

Table 33: Cost per job scenarios (minimum scenario: 71 Jobs)

Measure	Value (£)	Calculation
Nominal actual spend per job	137,933	£9,793,238 ÷ 71
Allocated budget per job	197,888	£14,050,073 ÷ 71
Real spend (2024/25 prices) per job	157,717	£11,197,940 ÷ 71

Source: Programme expenditure figures from DSIT financial records and CyberASAP allocated budget documents; employment estimates derived from Innovate UK data

Table 34: Cost per job scenarios (maximum scenario: 89 Jobs)

Measure	Value (£)	Calculation
Nominal actual spend per job	110,036	£9,793,238 ÷ 89
Allocated budget per job	157,866	£14,050,073 ÷ 89
Real spend (2024/25 prices) per job	125,820	£11,197,940 ÷ 89

Source: Programme expenditure figures from DSIT financial records and CyberASAP allocated budget documents; employment estimates derived from Beauhurst data

6.4.1.3 Net Investment Leverage Ratio

This ratio compares investment attracted (after a 70% attribution) with the adjusted programme spend. With a total nominal investment of £40m, the attributed investment is:

- Attributed Investment = £43,907,000 × 0.70 ≈ £30.74m

Thus, the leverage ratios are:

- Gross Investment Leverage Ratio = 43,907,000 ÷ 11,197,940 ≈ 3.92
- Net Investment Leverage Ratio = 30,735,000 ÷ 11,197,940 ≈ 2.74

Table 35: Investment leverage ratio

Investment measure	Value (£)	Calculation
Total real-terms investment raised	43,907,000	From Table 17
Real programme spend	11,197,940	From Table 51
Gross investment leverage ratio	3.92	43,907,000 ÷ 11,197,940
Attributed investment (70%)	30,735,000	43,907,000 x 0.70
Net investment leverage ratio	2.74	30,735,000 ÷ 11,197,940

Source: Nominal investment data from CyberASAP internal KPI documents, adjusted with ONS deflator data and stakeholder-derived attribution factors informed by the UK Government Additionality Guide and BIS analysis papers

6.4.2 Additionality of support

The survey data directly addresses the question of deadweight, or how much of the observed outcomes might have happened without the programme, by asking respondents to quantify how much of the quantifiable benefits can be attributed to CyberASAP. However, the number of beneficiaries who have generated meaningful economic benefits is relatively small, and the sample reporting estimates of deadweight in the survey is low. As such, these estimates should be treated with caution.

Attribution of benefits to CyberASAP

Our analysis acknowledges that not all outcomes can be credited to CyberASAP. Drawing on survey evidence and industry benchmarks, we have adopted a conservative 70% attribution factor. This factor implies 30% of the benefits (in terms of job creation, GVA, and investment) represent deadweight – outcomes that would have occurred irrespective of the programme. Although the UK government additionality guide reports deadweight ranges between 26-46% for business support programmes[53], our assumption reflects both stakeholder input and cautious approach.

Displacement, leakage, and sector considerations

Displacement and leakage are critical issues in evaluating additionality. It was not possible to source displacement data directly from participant surveys therefore evidence from the Government Additionality Guide for targeted business support interventions has been used where displacement of jobs would be expected to be around 42%. At the spinout stage, leakage is expected to be minimal since CyberASAP directly creates spinouts and generates employment within the UK. However, at the point of exit – such as buyouts or when companies are acquired – some leakage may occur as benefits are potentially reallocated to external markets or regions. Moreover, we consider the possibility of sector leakage. Cyber innovations are inherently sector agnostic. For instance, if a finance company invests in cyber, the investment still reflects a cyber capability, even if the benefits accrue in the finance sector. In our analysis, we assume that, for the current evaluation, sector leakage is not a primary concern given that most spinouts and employment outcomes occur in the UK. Nonetheless, we note that leakage may become more relevant at later stages, and further analysis will be required when exit events occur.

[53] Most recent version archived at GOV.UK. (2014). *Additionality Guide*

Sensitivity analysis

To assess the robustness of our evaluation, we conducted a sensitivity analysis on key assumptions that directly affect our outcomes. We varied the attribution factor, leakage ratio, multiplier, and employment estimates. For example, lowering the attribution factor (from 70% to 60%) reduces the number of attributable jobs and increases the cost per job, while a higher leakage ratio (from 30% to 40%) diminishes the net additional GVA. Similarly, adjusting the multiplier (from 1.5 to 1.75) proportionately scales the net additional GVA. The employment estimate—whether using a minimum figure (e.g., 102 employees from verified spin-outs) or an aggregated figure (127 employees from Beauhurst data)—directly influences all cost-effectiveness calculations.

Table 36: Sensitivity analysis – impact of key assumptions

Parameter	Base value	Low value	High value	Impact on outcomes
Attribution factor	70%	60%	80%	Lower attribution reduces attributable jobs, leading to a higher cost per job; higher attribution increases net benefits.
Leakage ratio*	30%	20%	40%	Higher leakage reduces net additional GVA and employment benefits; minimal leakage is assumed at the spin-out stage.
Multiplier	1.625	1.5	1.75	A higher multiplier directly increases net additional GVA, while a lower multiplier reduces the overall benefit.
Employment estimate	127	31	127	Using the conservative (lower) employment estimate increases the cost per job; net benefits scale proportionally with employment numbers.

*Source: Leakage and attribution benchmarks from the UK Government Additionality Guide (2014), BIS analysis papers, OECD reports, and insights from internal stakeholder discussions. *Note: Leakage at the spin-out stage is assumed to be minimal, although leakage may increase at later stages such as upon exit or acquisition.*

Bringing these additionality considerations together, we can provide a calculation of net additional jobs, GVA, and cost-effectiveness under typical assumptions for deadweight, displacement, leakage, and multiplier effects. For example, using:

- Gross Employment: 127
- Attribution Factor[54]: 70%
- Displacement[55]: 42%
- Leakage[56]: 10%
- GVA per Employee[57]: £116,200

[54] Derived from survey data and stakeholder inputs in conjunction with guidance from the UK Government Additionality Guide (2014) indicating typical deadweight ranges for business support programmes.
[55] Midrange figure from the UK Government Additionality Guide for targeted business support interventions.
[56] Reflects minimal expected leakage for spin-outs at an early stage (further references include local programme data and stakeholder interviews)
[57] Sourced from the Cyber Security Sector Analysis 2025

- Multiplier (High-Tech Tradable)[58]: 1.625
- Adjusted Programme Cost[59]: £9.79 million

We arrive at:

1. Net Additional Jobs
   - After deadweight (70% attribution): ~89
   - After displacement (42%): ~52
   - After leakage (10%): ~47
   - Including multiplier (x1.625): ~76
2. Net Additional GVA (Annual)
   - Direct GVA: 47 × £116,200 ≈ £5.46 million
   - Including multiplier (×1.625): ~£8.89 million
3. Cost per Net Additional Job = £11.20 million/76 ≈ £147,000. This represents the lifetime programme cost per job.
4. To produce an annual measure, we spread the total real cost (~£11.20 million) over an eight-year delivery period, yielding ~£1.40 million average annual cost. Annual GVA-to-Cost Ratio = £8.89 million / £1.40 million ≈ 6.35

Under these assumptions, CyberASAP has generated approximately 76 net additional jobs, and is currently responsible for £8.89 million in annual GVA after accounting for deadweight, displacement, and leakage. The ratio of annual recurring GVA to annual programme cost is currently about 6.35:1. Over time, if spin-out jobs persist and grow, the cumulative economic return will improve accordingly.

6.5. NAO "4'E's" value for money assessment

Return on investment would be the preferred metric for value for money if all benefits were readily quantifiable and if the programme were sufficiently mature for long-term economic benefits to have arisen. However, since the most recent cohorts are yet to produce revenue-generating spin-outs, we have used the National Audit Office's "4 'E's" methodology, which can be used on both qualitative and quantitative data to assess the value for money of the programme to date across four standard dimensions:

- Economy: **spending less** by minimising the cost of resources used or required (inputs)
- Efficiency: **spending well** by managing the relationship between the output from goods or services and the resources to produce them;
- Effectiveness: **spending wisely** by comparison with the intended results of public spending (outcomes)
- Equity: **spending fairly** as judged by the degree to which the results of the intervention are equitably distributed.

We have assessed these "4'E's" by examining each criterion using a scoring rubric and sub-criteria designed specifically for the programme.

[58] Representative value from the HMT Green Book for high-tech/tradable sectors (often cited for advanced manufacturing and R&D-intensive activities).
[59] Real Programme Cost (2024/25 prices) – £11.25 million (derived from DSIT financial records and ONS GDP deflator data).

To ensure transparency and consistency in our VfM judgements, we have developed a set of tailored performance standards for each of the 4E dimensions. These standards outline the evidence thresholds associated with different levels of performance—ranging from Poor through Excellent—and serve as the foundation for our ratings of CyberASAP. For a detailed explanation of these sub-criteria, indicators, and how each level of performance is defined, please refer to Appendix F – 4E Framework with Tailored Performance Standards.

6.5.1 Economy

Definition (Economy): CyberASAP uses its available resources in a cost-conscious manner—minimising spend on overheads, administration, and delivery while maintaining sufficient quality of support for participants.

Sub-criteria:

- **Financial management** – Does the programme remain within budget, recycle underspend effectively, and handle grant administration prudently?
- **Procurement & governance** – Are internal checks (e.g. panel reviews, TTO involvement, volunteer mentors) organised to avoid duplication or inflated costs?
- **Adaptability in design** – Does the programme respond cost-effectively to new challenges (e.g. switching some activities online) to reduce overheads while maintaining quality?

Table 37: Economy – sub-criteria, evidence, and performance standard

Sub-criteria	Evidence	Performance standard
Financial management	CyberASAP's actual spend is less than the total amount DSIT budgeted for the programme. Expenditure on grants is released in phases only after outputs are verified, which promotes prudent disbursement. Any budget not spent currently reverts to DSIT, ensuring the programme does not exceed its budget and maintains cost controls.[60]	**Good**
Procurement & governance	The process evaluation (section 4) describes robust panels and TTO involvement in gating decisions, reducing the risk of misallocated funds. Mentors are often volunteers who provide expertise without direct cost, though the scale of these volunteer contributions is not extensively quantified. These features, together with risk management checks before each phase, help avoid inflated or duplicate spending.	**Partial–Good**
Adaptability in design	The programme adopted online and hybrid delivery from 2020 onward, effectively lowering travel and event overhead without reducing participant satisfaction. The phased model focuses resources on strong teams, so fewer low-potential projects are carried forward, thereby containing costs. Overall, these adaptations illustrate the programme's cost-effective response to emerging challenges.	**Good**

CyberASAP achieves **"Good"** economy. It balances an inherently hands-on support model with prudent financial controls. Programme cost efficiencies have helped contains expenditure. Underspends are reallocated (toward programme enhancements, such as mentor support and additional advisory engagement) or returned subjected to DSIT approval, overhead is lean, and adaptive design (online

[60] It should be noted the DSIT budget for CyberASAP is the maximum available and not what InnovateUK/programme participants are expected to spend. Therefore, the difference between this figure and the actual spend is not considered 'underspend' by DSIT.

mentoring) contains costs. Some mild duplication arose with new industry strands; however the programme remains cost-conscious.

6.5.2 Efficiency

Definition (Efficiency): CyberASAP maximises productivity by delivering the intended scope and volume of outputs—proofs of concept, market-validated value propositions, and spinout-ready teams—using the fewest possible inputs of time, funds, and staff.

Sub-criteria:

- **Coverage & reach** – Does the programme engage enough universities, departments, and academic teams to ensure broad coverage?
- **Quality of outputs** – Are the end-stage pitches, PoCs, and spinout teams sufficiently advanced for genuine commercial viability?
- **Process & time management** – Are the phased gating, mentor sessions, and TTO interactions orchestrated to minimise wasted effort while maintaining throughput?

Table 38: Efficiency – sub-criteria, evidence, and performance standard

Sub-criteria	Evidence	Performance standard
Coverage & reach	Section 4 outlines the number of projects increasing across cohorts, and how communication/promotion broadened awareness among Russell Group and post-92 universities. It also shows that online delivery enhanced geographic access, especially for those unable to travel often, thereby extending the programme's reach across multiple regions.	**Good**
Quality of outputs	The selection panels are effective at making sure that only high-quality projects pass through the '*stage gates*' to later phases. As a result, most Phase 2 teams produce credible proofs of concept that are regarded as investor-ready by alumni and TTOs. Participants' demos and final pitches have been through an advanced level of market validation for the viability of their proposed solutions, although deep-tech areas sometimes require more specialised mentors.	**Partial–Good**
Process & time management	The phased approach channels resources to the most promising ideas, minimising wasted effort. Participant feedback suggests scheduling and planning are generally effective, though a few academics with large teaching loads found the pace challenging. On balance, it manages throughput well.	**Good**

CyberASAP is **"Good"** in efficiency. It delivers a robust pipeline of outputs—value propositions, PoCs—via staged gating that maximises use of limited staff/mentor time. Hybrid sessions extend coverage efficiently, though advanced or deep-tech teams note partial mismatch in mentor expertise.

6.5.3 Effectiveness

Definition (Effectiveness): CyberASAP successfully achieves its intended outcomes—accelerating the commercialisation of UK academic cyber security research—resulting in new spin-outs, viable cyber products, and increased investor interest.

Sub-criteria:

- **High rate of spin-out/startup formation** – Do the final teams actually create spin-outs/licences within ~12–24 months post-programme?
- **Enhanced investment & market entry** – Are participants attracting VC/angel backing and/or launching genuine cyber products?
- **Improved commercial awareness & skills** – Have participants grown their entrepreneurial mindset, TTO engagement, and investor pitching ability?

Table 39: Effectiveness – sub-criteria, evidence, and performance standard

Sub-criteria	Evidence	Performance standard
High rate of spin-out/startup formation	Multiple spinouts (30+ overall) and licensing routes have emerged. TTOs confirm that CyberASAP accelerates concept-to-spin-out timelines by instilling commercial rigour early. However, not all projects aim for spin-out; some prefer licensing or open-source.	**Good–Excellent**
Enhanced investment & market entry	There has been ~£40 million in total external investment, with single spinouts sometimes raising £2–3m. Investors interviewed point to the strong pitch training and improved PoC quality. Most participants from earlier cohorts (1–5) who pursued external funding successfully raised capital (albeit at varying scales).	**Good**
Improved commercial awareness & skills	Survey data suggests there has been substantial increases in participants' self-assessed commercial capabilities (from ~4/10 to ~8/10), and interviews reinforce that many only gained investor readiness and IP strategy knowledge through CyberASAP. TTOs confirm a mindset shift toward market-driven thinking.	**Good**

CyberASAP's outcomes are **"Good–Excellent"** overall. Notable spin-out creation, multi-million follow-on investments, and participant testimonies show real success in commercial readiness. External factors like TTO IP policies do matter, but the consistent results across cohorts confirm strong effectiveness.

6.5.4 Equity

Definition (Equity): CyberASAP ensures that opportunities and benefits (e.g., spin-out success, skill-building, funding) are fairly distributed across diverse universities, regions, and researcher demographics—no key group is left behind.

Sub-criteria:

- **Inclusive participation** – Are diverse universities, female/ethnic-minority academics, and varied regions engaged?
- **Fair distribution of benefits** – Does the spin-out success or follow-on funding concentrate in just top Russell Group unis?
- **Accessibility of support** – Are face-to-face vs. online sessions, TTO resources, volunteer mentors accessible to all?

Table 40: Equity – sub-criteria, evidence, and performance standard

Sub-criteria	Evidence	Performance standard
Inclusive participation	Section 4 shows how communication and promotion broadened the applicant pool to include post-92 and smaller institutions. There has also been an increasing share of female and ethnic-minority participants, though still below parity.	Partial–Good
Fair distribution of benefits	Spinouts and licensing deals now arise from multiple university types, not only top-tier ones. Post-92 universities are more active than at the programme's outset. However, Russell Group universities do still secure a notable share of spin-out activity.	Good
Accessibility of support	The shift to hybrid sessions after 2020 and the TTO webinars have made it easier for distant participants to engage. Yet some events remain London-based, which can still be challenging for those with family or caring responsibilities.	Good

CyberASAP meets **"Good"** equity standards. It proactively broadens participation to smaller/regional universities, and the female-led academic share is improving though still short of parity. Many post-92 unis see real commercial gains. Extra support for TTOs with limited capacity, plus targeted outreach to underrepresented groups, may further enhance equity.

7. Benchmarking

This section summarises key findings from three selected international comparator programmes, as well as best practice spinout programmes in the UK. It includes key learnings gained from these comparators to inform future iterations of CyberASAP.

7.1. Summary of key findings

This section highlights key learnings from international and UK comparator programmes that can inform future iterations of CyberASAP. These include the importance of involving TTOs to facilitate spinouts and improve the commercialisation process of projects. Programmes such as the ON Program in Australia and the ICURe Programme support TTOs by alleviating resource constraints, improving project management, and enhancing networking skills.

Follow-on support is crucial for the sustainability and success of projects. The ON Program provides six-month post-programme support, while UKRI's ICURe Programme and Connecting Capability Fund (CCF) offer mentorship, networking opportunities, and access to industry experts to sustain momentum and overcome challenges. CyberASAP could consider extending its support duration and adopting these strategies to enhance the sustainability of its outcomes.

Market validation through early engagement with customers and stakeholders is also emphasised. Programmes like ICURe, Cyber Security Innovation Network (CSIN) and the ON Program encourage teams to use customer interviews, surveys, and pilot testing to refine business models and align projects with market needs.

Collaboration between industry and academic institutions is also a key finding. CSIN fosters this collaboration through work-integrated learning programmes, co-op programmes, apprenticeships, internships, and practicums. This approach could be beneficial for CyberASAP to enhance industry-academia collaboration and cyber talent development.

However, there are challenges in comparing CyberASAP with international programmes due to the lack of up-to-date, relevant data. While UK-based programmes such as the Commercialising Quantum Technologies Challenge, CCF, and ICURe have extensive data available, international programmes like CSIN and Transition to Practice (TTP) have limited formal evaluations.

7.2. International comparator programmes

7.2.1 Comparator countries

Many international programmes support the commercialisation of cyber security research and development (R&D). In the United States, major investments in R&D have resulted in large clusters of cyber security firms in Silicon Valley, Washington D.C, Boston, the New-York tri-state area, and the San Antonio-Austin corridor[61]. Singapore has positioned itself as a cyber security hub in Asia, with the Cyber Security Agency of Singapore supporting research commercialisation through various grants and programmes[62]. Other countries, including Australia, Canada, France, and Germany, have implemented interventions to support R&D and commercialisation of cyber security and related technologies.

[61] B1_5__KTN_USA-Cybersecurity.pdf (Accessed 25/02/2025).
[62] Cyber Security Agency of Singapore (Accessed 24/01/2025).

For this report, we benchmark CyberASAP against government-funded interventions that support the commercialisation of cyber security R&D in three comparator countries: TTP[63] in the United States, CSIN[64] in Canada, and the ON Program[65] in Australia. The United States was chosen for comparison as the leading country globally for the commercialisation of cyber security spinouts, offering valuable insights. Canada and Australia were chosen as comparators because they are English-speaking countries, ensuring the accessibility of documentation and evidence sources for our review; have similar-sized economies to the UK, allowing for valuable comparisons; and they have reputable higher-education institutions (HEIs).

A detailed summary of each country and its programmes is detailed in Appendix C.

7.2.2 Context in which programmes are offered

This section provides context for each country in which the comparator programmes are/were delivered.

The United States is considered the leading player in the global cyber security sector. In 2023, the United States' cyber security market was valued at $67.69 billion[66] (approximately £54.42 billion[67]), notably larger than the UK's market, which was valued at £11.9 billion in the 2022-23 financial year. The federal government invests over £1 billion annually in unclassified cyber security research, though only a small fraction reaches the market. This gap, known as the 'Valley of Death', often results from insufficient collaboration between the government and the private sector, limited resources, and inefficient technology transfer processes[68]. The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) aimed to bridge this gap within the cyber security sector between 2012 and 2019 through the **TTP programme**.

Key players in the United States' cyber security sector include government agencies (e.g. the Office of the National Cyber Director (ONCD), DHS and the Defense Advanced Research Projects Agency), academic institutions (e.g. Massachusetts Institute of Technology (MIT)'s Computer Science and Artificial Intelligence Laboratory (CSAIL) and Carnegie Mellon University's CyLab), private companies (mainly focused in the five geographical clusters mentioned in section 7.1.1), and non-profit organisations.

Canada's cyber security industry contributed CAD 3.2 billion (approximately £1.86 billion[69]) to GDP in 2020, with high R&D intensity, mostly funded by private industry[70]. Key players in supporting R&D and the commercialisation of cyber security technology in Canada include Innovation, Science and Economic Development Canada (ISED), the National Cybersecurity Consortium (NCC) Canada, the Canadian Institute of Cybersecurity (CIC), and CANARIE.

One of Canada's National Cyber Security Strategy[71] key pillars is to make Canada a global leader in innovative cyber technology, through which many initiatives are being delivered. Funded by ISED, the NCC is delivering **CSIN**, which aims to improve R&D, increase commercialisation, and support the development of cyber security talent across Canada.

Australia's cyber security industry contributes over AUD two billion (approximately £1.07 billion[72]) to GDP annually. By 2030, the Australian Government aims to become a world leader in cyber security, as outlined

[63] TTP | Homeland Security (Accessed 25/02/2025).
[64] Cyber Security Innovation Network - Cyber Security Innovation Network (Accessed 03/02/2025).
[65] It's ON: Innovation Program for Researchers - CSIRO (Accessed 25/02/2025).
[66] U.S. Cybersecurity Market Size | Industry Report, 2030 (Accessed 25/02/2025).
[67] Based on the average conversion rate of 1 USD to 0.8042 GBP in 2023.
[68] TTP—Transition to Practice Technology Guide (Accessed 25/02/2025).
[69] Based on the average conversion rate of 1 CAD to 0.5814 GBP in 2020.
[70] State_Cybersecurity_eng_0.pdf (Accessed 03/02/2025).
[71] National Cyber Security Strategy (Accessed 25/02/2025).
[72] Based on the average conversion rate of 1 AUD to 0.5344 GBP in 2023.

in their Cyber Security Strategy Action Plan 2023-30[73]. Key players in supporting R&D and the commercialisation of cyber security technology in Australia include the Cyber Security Cooperative Research Centre (CSCRC), AusIndustry, Commonwealth Scientific and Industrial Research Organisation (CSIRO) and the Academic Centre of Cyber Security Excellence (ACCSE).

CSIRO is delivering the **ON Program** which focuses on supporting researchers to translate their ideas from academia to commercialisation. Although not specific to cyber security, the ON Program has supported many teams developing cyber security and related products and services. A unique challenge in Australia is university leaderships' focus on IP and commercialisation as revenue streams. This results in universities typically retaining a sizable equity share (30-50%) in spinout companies, which is higher than international comparisons. Consequently, negotiations between research founders and universities are often challenging, delaying timely spinouts. CSIRO aims to address this issue with the ON Program through strong involvement of university Technology Transfer Offices (TTOs) in the programme[74].

7.2.3 Support provided

7.2.3.1 Programme objectives

TTP and CSIN share similar objectives with CyberASAP, aiming to support the development and commercialisation of cyber security technologies. They focus on encouraging collaboration between academia, industry, and other partners to achieve their goals. These programmes are driven by national cyber strategies guiding their design and implementation. For example, TTP focuses on identifying technologies that address the United States' national security needs, including funding some defence-related projects, while CyberASAP explicitly excludes defence-related projects. CSIN focuses on diversifying Canada's cyber security sector by strengthening the talent pipeline and promoting projects across various geographical regions, thereby enhancing the pan-Canadian network.

The ON Program differs slightly in terms of its objectives, focusing instead more broadly on the commercialisation of wider technology outside of cyber security. However, this programme aligns in terms of its objectives of fostering collaboration between academia and industry in Australia.

7.2.3.2 Programme delivery

CyberASAP and its comparator programmes support annual cohorts of projects with non-repayable grant funding aimed at developing and commercialising cyber security technologies. Alongside the grant funding, the programmes offer training, mentoring, and opportunities to showcase technologies, such as through technology demonstration days. The primary focus of these programmes is to help projects develop, validate, and test their products and services.

Despite the alignment of these programmes, they differ greatly in terms of structure, timelines, and the size of grants offered to projects:

- Between 2012 and 2019, the TTP supported annual cohorts of approximately eight projects, totalling over 60 technologies over the lifetime of the programme, considerably fewer than the 170+ projects supported by CyberASAP in a similar timeframe. Each TTP project was supported over a 36-month period, three times longer than CyberASAP, with technology validation, testing, evaluation, and pilot deployments. Similar to CyberASAP, TTP featured Technology Demonstration Days to connect researchers with investors and potential licensors. The amount of funding received by each TTP project is unknown but is

[73] 2023-2030 Australian Cyber Security Strategy (Accessed 24/01/2025).
[74] Interview with CSIRO representative involved in delivering the ON Program.

assumed to be greater than that of CyberASAP (maximum of £92,000) based on high-level financial figures available[75].

- CSIN has funded 56 projects across two annual Calls for Proposals in 2023 and 2024, with each project focusing on either commercialisation, R&D, or training. On average, CSIN projects receive approximately CAD 607,721 (approximately £328,169.34[76]) in funding, significantly more than CyberASAP projects. CSIN activities resemble those of CyberASAP, but the programme places a greater emphasis on skills development to address skills gaps, developing educational pathways, and supporting curriculum development. Additionally, CSIN projects must commit 1:1 match funding of the ISED investment, unlike CyberASAP which requires no match-funding from projects.
- Similar to CyberASAP, the ON Program is structured in two separate programmes: a pre-accelerator (ON Prime) and accelerator programme (ON Accelerate). ON Prime focuses on very early-stage ideas, helping researchers identify their customers and the problems they aim to solve through a six-day hybrid programme over nine weeks, offering coaching, one-to-one mentoring, and a showcase event. ON Accelerate is designed for creating new deep-tech ventures. It begins with a two-day selection bootcamp, followed by an immersion week, and then a three-month programme with coaching and mentoring. It concludes with a showcase event and offers up to six months of ongoing coaching post-programme. It is anticipated that around 100 teams each year between 2022 and 2026 will access the ON Prime programme, with some progressing on to ON Accelerate. Over the course of the two programmes teams can receive up to AUD 85,000 (approximately £41,650[77]), just under half of the CyberASAP maximum funding amount.

7.2.4 Key outcomes

7.2.4.1 Intended/expected outcomes

TTP and CSIN share many expected outcomes with CyberASAP, including increased commercialisation of cyber security R&D, increased number of cyber security startups and spinouts, viable cyber security products or services, patents, and improved collaboration between industry and academic institutions. They also aim to improve the skills and knowledge within the cyber security sector and expand the workforce in cyber-related fields. The ON Program aligns with these aims but does not solely focus on the cyber security sector, instead funding health, energy, agriculture, and manufacturing as well.

There are some differences in intended outcomes and impacts of CyberASAP and the comparator programmes:

- Due to its focus on addressing the cyber security needs that affect the United States' national security, TTP's expected outcomes are aligned accordingly, with many of the technologies intended for government use, including by the DHS. CyberASAP does not require such alignment with national security needs.
- CSIN places greater emphasis on collaboration between industry and academic institutions from the outset, requiring joint involvement in consortium projects. This results in outcomes related to collaborative efforts and increased participation of post-secondary students in work-integrated learning programmes established by the network. CSIN also explicitly references Technology Readiness Levels (TRLs) in their outcomes, aiming for projects to advance by at least two TRLs.

[75] The TTP programme has leveraged over $250 million in funding from other federal agencies (including Department of Energy National Labs and Federally Funded Research and Development Centres) across just over 60 technologies.
[76] Based on the conversion rate of 1 CAD to 0.54 GBP (18/03/2025).
[77] Based on the conversion rate of 1 AUD to 0.49 GBP (18/03/2025).

- The ON Program supports the development of earlier-stage ideas through ON Prime before focusing on commercialisation in ON Accelerate. For example, it helps teams to improve their clarity around the impact and focus of their research and identify their customer and the specific problem they are solving through market research with potential industry customers. Much like CyberASAP, this is an opportunity for projects to test and refine their value proposition, ensuring that the product or service has an addressable market before commercialisation activities.
- CyberASAP and TTP seem to place more emphasis on broader commercialisation impacts of R&D, with TTP specifically aiming to improve the long-term ability of federal government research organisations to transition technology more efficiently, and the UK programme aiming for the wider commercialisation of academic research and ideas. CSIN and the ON Program do not mention this aspect.

7.2.4.2 Observed outcomes[78]

TTP: Since its inception in 2012, TTP has facilitated the launch of seven new startups (see 7.1.5 for examples) and the successful transition of 21 technologies, five of which were made available as open-source software. Comparatively, CyberASAP has a slightly higher success rate, supporting the formation of 32 startup companies from 170 projects, equating to 19%, compared to 12% for TTP. This could be attributed to the fact that many TTP technologies are defence-related, which are generally more challenging to spinout. This is due to several reasons, including regulatory hurdles and lower investment opportunities outside of the public sector[79].

Examples of open-source software facilitated by TTP include:

- AMICO (Accurate Malware Identification by Classification of live network traffic Observations) developed by researchers at the University of Georgia in 2015, in use by universities.
- Hone (Host and Network Data Correlation technology) developed by the Pacific Northwest National Laboratory (PNNL)80 in 2015, actively used by Google and others.
- SCOT (incident response threat intel technology) developed by the PNNL in 2015, in use by the United States government.

Additionally, LOCKMA (Lincoln Open Cryptographic Key Management Architecture) developed by MIT Lincoln Laboratory through TTP to address the complex problem of cryptographic key management was recognised in by the prestigious 2012 R&D 100 award and won the MIT Lincoln Laboratory Best Invention Award.

The ON Program: Since its inception in 2015, the ON Program has supported the creation of over 70 companies and has created over 700 new jobs. Participants have attracted AUD 320 million (approximately £156.8 million[81]) in commercialisation grants and AUD 36.4 million (approximately £17.84 million) in private capital. CyberASAP in contrast has attracted £40 million in further funding from sources including seed funding, venture capital (VC) and angel investment.

[78] As most CSIN projects had a start date of 2024, it is too early to assess the outcomes of the funded projects. Future updates on project impact and outcomes can be found on the NCC's website (https://ncc-cnc.ca/).
[79] Full article: Technology transfer and defence sector dynamics: the case of the Netherlands (Accessed 26/02/2025).
[80] A United States Department of Energy national laboratory which conducts research in energy, national security, and the environment in Washington State University and other academic institutions.
[81] Based on the conversion rate of 1 AUD to 0.49 GBP (18/03/2025).

From their first phase of the programme (2016 to 2019) **CSIRO** reports that the programme had a '*commercial conversion rate*' of 55%, whereby an idea is turned into a startup company, substantially higher than CyberASAP and other comparator programmes[82].

A CSIRO representative attributes much of their success to their showcase events where projects have the platform to showcase their work to and network with high-calibre investors, including VCs and angel investors. The showcase event at the end of ON Prime is particularly important, as it allows investors and stakeholders to then track the teams' progress throughout ON Accelerate, building trust and interest in the ventures, which can lead to further investment.

The six months of post-program coaching provide funding and support to help teams determine their next steps, such as joining other accelerators or securing additional funding. This extended support has been instrumental in guiding teams through critical early stages, ensuring they have the resources and mentorship needed to progress effectively.

7.2.5 Examples of spinouts

The comparator programmes have resulted in numerous spinouts, including the following:

- **ZeroPoint** (weaponised document detection technology) is a spinout from TTP. Developed by researchers at the University of North Carolina at Chapel Hill and funded by the National Science Foundation, it was the eighth cyber security technology to transition to commercialisation through TTP. ZeroPoint Dynamics now has a core team of six employees and offers services to DHS and the Defense Advanced Research Projects Agency[83].
- **PEACE** (Policy Enforcement and Access Control for Endpoints technology) was developed at the Worcester Polytechnic Institute and is a spinout from TTP. The technology, which protects endpoint devices by intercepting all new network connections and vetting them at a centralised network controller, was spun out by the Massachusetts-based startup ContexSure Networks, Inc.
- **Medivox** by Supanova Health is an AI-powered digital platform that delivers reliable and accessible interpretation tailored for healthcare settings. Cyber security and data protection is a core functionality of the tool. Medivox started in 2023 during the Perth Biodesign course and in 2024 the team behind Medivox, led by the Australian National University, participated in Cohort 15 of ON Prime[84]. In January 2025, Medivox were successful in receiving a ~£100,000 grant from the Cook Government's Innovation Solutions – Digital Health funding programme[85].
- There are many notable graduates from the ON Program including **Emesent** (raised AUD 2.5 million/£1.23 million), **Ynomia** (raised AUD 3.6 million/£1.76 million), **RapidAIM** (raised AUD 1.25 million/£612,500) and **Presagen** (raised AUD 4.5 million/£2.21 million)[86]. Although these spinouts are not directly related to cybersecurity, this demonstrates the success of the programme in supporting academics commercialise their research more widely.

7.3. UK programmes

CyberASAP is part of a broader ecosystem of cyber security growth and innovation programmes, as detailed in section 3.3. It is complemented by other government and private sector initiatives within wider

[82] CSIRO to shutter ON startup program
[83] https://www.zeropointdynamics.com/ (Accessed 18/03/2025).
[84] ON Alumni – CSIROpedia (Accessed 03/02/2025).
[85] New funding backs local researchers to harness AI in healthcare | Western Australian Government (Accessed 03/02/2025).
[86] CSIRO to shutter ON startup program (Accessed 18/03/2025).

commercialisation programmes aimed at helping academics and private sector partners spin out, as illustrated in the following table.

Table 41: Mapping of other commercialisation programmes

Programme	Programme description	Outcomes
UK Research and Innovation (UKRI) Commercialising Quantum Technologies Challenge (2018 to 2025)[87]	**Funding:** UKRI is investing £174 million, supported by £390 million from industry. **Target group:** Companies and projects involving products/technologies based on advances in quantum science. This competition aims to advance the commercialisation of new products and technologies in quantum science across sectors including cyber security, infrastructure, and healthcare. It supports the UK quantum industry through four areas: product and service innovations, industry-led projects, supply chain feasibility projects, and an investment accelerator.	In 2023, projects, with £204 million of allocated funding had generated £513 million of private investment, equating to £2.51 for every £1 of UKRI investment. Projects developed 80 new or improved products, nine new or improved services, and nine new or improved processes. They generated or supported more than 1,800 jobs, of which 1,470 were high-skill[88].
UKRI Connecting Capability Fund (CCF) (First Phase: 2017 – 2023, Second phase: ongoing) [89]	**Funding:** Research England's CCF programme invested £111 million. **Target group:** Higher education providers and their collaborations with private sector partners. The CCF programme supports higher education providers commercialise their research and promotes collaborations between universities and private sector partners. It has funded accelerator programmes and developed venture funds like Northern Gritstone and Midlands Mindforge. Common objectives include developing spinout companies and start-ups, creating university venture funds, enhancing IP licensing, strengthening business partnerships, and developing technology clusters.	The first phase of CCF resulted in 214 new spinouts, 338 new products and services launched, and 12,969 people trained in enterprise skills. For every £1 invested by Research England, projects leveraged £7.70. Projects brought in combined supplementary funds of £391 million, additional support of £149 million for individual spinouts, and £315 million for investment funds[90].

[87] Commercialising quantum technologies challenge – UKRI (Accessed 26/02/2025).
[88] IUK-UKRI-291123-CommercialisingQuantumTechnologiesChallenge.pdf (Accessed 26/02/2025).
[89] Connecting Capability Fund – Research England Development Fund – UKRI (Accessed 26/02/2025).
[90] Microsoft Word - CCF final evaluation - final 2024-10-11 (Accessed 26/02/2025).

Programme	Programme description	Outcomes
Innovate UK Innovation-to-Commercialisation of University Research (ICURe) Programme (2013 – 2018)	**Funding:** ICURe cost £18.2 million, covering both the costs of delivering the programme and the start-up aid provided to some teams through Aid for Start-Ups and Follow-On Funding. **Target group:** Research teams in UK universities comprised of researchers, business advisors, and TTOs. The ICURe programme, established in 2013, addressed commercialisation failures in academic research by providing funding and training. It also offered grants to teams advised to create spinouts, effectively providing seed capital to accelerate company growth.	35% of participating teams founded spinouts, compared to 12% of non-participants. Without ICURe, an estimated 49 to 55 spinouts would not have been incorporated. Spinouts established by the participating teams raised external equity investment, averaging £839,000 per company. The average valuation of spin-outs established by participating teams was £1.3 million. Spin-outs created an average of 2.75 jobs per company, leading to an estimated 122 to 127 gross additional jobs[91]. 6% of participating teams secured licensing agreements.

[91] Normal dot (Rev02 January 2009) (Accessed 26/02/2025).

8. Conclusions and Recommendations

This section outlines conclusions based on the evidence collected against the evaluation questions and includes recommendations to inform future programmes.

8.1. Process evaluation

This section sets out the conclusions against the research questions. It includes recommendations that could make the programme more effective.

8.1.1 To what extent was the programme delivered as intended?

The programme has been successfully delivered as intended. Almost all milestones were delivered as planned. The exceptions to this were delays to delivery of milestones relating to the confirmation of the sixth and seventh years of the programme and Year 6 and 7 competition promotion, publishing, opening, and closing. These delays are the result of Innovate UK needing to wait for government to confirm the availability of funding. They have not, however, had negative impacts on the delivery of the programme.

8.1.2 What worked well, or less well, for whom and why?

8.1.2.1 CyberASAP worked well with regard to:

- The hands-on approach provided by KTN/Innovate UK Business Connect which helped the teams progress through the programme. The quality of support and the knowledge of KTN/Innovate UK Business Connect, Plexal, trainers and others received very positive feedback. This resulted in high participant attendance levels at events, training, and bootcamps.
- The collaboration between KTN/Innovate UK Business Connect, Innovate UK and DSIT/DCMS to update the design of CyberASAP over time to reflect feedback from participants and other stakeholders. Most recently this included additional activities to engage with alumni after they graduate from the programme and to engage with potential applicants before the programme. These additional activities help alumni continue to develop their projects and allow potential applicants to understand more about the programme, its aims, and its contents before they decide whether to apply. The activities address feedback from participants and stakeholders and were financed through the use of minor underspends, which usually occur in programmes like CyberASAP where academics have access to grant funding.
- The fast-paced delivery of the programme within one year and with multiple stage-gates determining progression of teams which contributed to high levels of participant engagement with the content of CyberASAP.

8.1.2.2 The areas that could be improved include:

- Setting out the expected time that academics will need to be able to get fully involved in CyberASAP. A small number of senior academics felt that the time required was not clear when they applied to CyberASAP and was difficult to manage when considering their teaching and research commitments. Academics from universities further away from London noted that travel time for in-person events can be a barrier, especially for those with family or care commitments.
- Providing more flexibility in the content and format of pitch presentations to assessment panels. This could suit projects with diverse backgrounds better than the standardised approach adopted to date.
- Ensuring that teams with ideas with no realistic application are not approved for the Programme. Panel members and trainers noted that teams occasionally participated whose ideas had no apparent realistic application.

8.1.3 Were there any unexpected or unintended issues with the delivery of the programme?

No unexpected or unintended issues were reported.

8.1.4 What can be learned from the delivery methods used?

The existing delivery methods are effective, particularly the delivery of the programme within one year, its focus on cybersecurity, the involvement of industry experts, panel members, trainers, Innovate UK and Plexal staff. The programme provides commercialisation knowledge (contributed by KTN/Innovate UK Business Connect and Plexal), cybersecurity industry knowledge (provided by panel members), and the specific business skills (from training providers). The combination of grant funding and delivery in successive phases helps academic teams focus on key aspects of commercialisation one after the other, giving the programme a well-functioning structure.

The in-person nature of training and other events also received mostly positive feedback, suggesting that in-person delivery is favoured over remote, online delivery. It allows for more effective training, learning, and networking. The downside of in-person delivery is the need for participants to travel, which can be a barrier particularly for those who have family or caring responsibilities.

8.1.5 To what extent did external factors influence the delivery and functioning of the programme?

External factors played only a limited role in the delivery of the programme. The factors that emerged were the repercussions of the COVID-19 pandemic and funding approved annually.

While the COVID-19 pandemic did not influence delivery of activities for Years 6 to 8 directly, delivery partners noted that projects funded during the pandemic had less exposure to investors and potential customers compared to projects funded outside the pandemic. Innovate UK mentioned this as a key factor driving the need for additional engagement activities with and tracking of alumni.

Government planning cycles, which tend to favour funding for programmes for one financial year, led to Innovate UK operating programme competitions at risk, before knowing whether DCMS/DSIT would fund the following year's activities. This has not led to any reported impacts on actual delivery because the programme has continued to operate. However, it is not realistic to assume Innovate UK can continue to operate at risk, and when this happens it will impact on programme timings.

8.1.6 Recommendations arising from the process evaluation

Recommendation 1. Innovate UK should continue to run the CyberASAP Pathfinder project so that potential applicants can understand the content of the programme and the extent to which it would be useful to them. It would be beneficial to seek feedback from CyberASAP Pathfinder participants to understand the extent to which the Pathfinder helps them decide whether to apply for CyberASAP, when to apply for CyberASAP, or make adaptations to their idea before they decide to apply to CyberASAP. Doing this will help ensure that the Pathfinder is useful to applicants so that academics can make the most of CyberASAP itself.

Recommendation 2. Participants should be required to book up to three events following the networking training to put what they learned into practice. After this, they should report back to Innovate UK and the trainer. This would ensure that participants start to build their network and put what they learn into practice while they are still part of the programme.

Recommendation 3. DSIT and Innovate UK should formulate more specific challenges for the industry challenge-led cohort. Specific business challenges could be more effective in achieving the desired

outcomes of CyberASAP than general themes. The challenges formulated for the industry challenge-led cohort in Year 8 were broad, representing themes such as cybersecurity supply chains.

Recommendation 4. DSIT, Innovate UK should consider whether participants can have more flexibility in the format and structure of their pitches to assessment panels, including for instance written submissions in addition to the presentation. Flexibility could allow teams to focus more on the strengths of their ideas while considering that some participants do not have English as their first language. Implementing this recommendation will require Innovate UK to support assessors with guidance on how to consistently score pitches despite varying format and structure.

Recommendation 5. Assessment panels in between phases could be strengthened through the inclusion of further technologically knowledgeable people such as Chief Information Security Officers, who can give reasoned feedback on the applicability and relevance of ideas to current challenges. Innovate UK would need to work with industry to encourage CISOs to take part in panels.

Recommendation 6. So that DSIT can assess the achievement of key outputs and outcomes in-year, rather than after the conclusion of each year of the programme, or through evaluations such as this one, evaluation recommends that monthly reporting should include further key outputs and outcomes of the programme, including the number of proof-of-concept demonstrators, new patents and technologies, and market validated value propositions.

8.2. Impact evaluation

This section provides conclusions against the research questions. It includes recommendations that could make the programme more effective.

8.2.1 To what extent has the programme been effective at enabling the academic sector to commercialise their ideas or speed up this process?

The programme has been highly effective in this regard. Academics have passed through the stages of the programme – defining a value proposition, carrying out market validation, and developing a proof of concept – and progressed to commercialisation through forming a spin-out company, or other routes such as licensing agreements.

Some of the key mechanisms through which CyberASAP acts are that it significantly raises the skills, knowledge, and confidence of academic teams to commercialise, it speeds up the transition from concept to spin-out, and it increases researchers' ability to secure investment.

8.2.2 What are the challenges facing academics upon graduation of the programme? To what extent has the programme been effective at mitigating these? How else might the programme support alumni/graduates?

Academics typically lack experience in making contacts with industry, and the programme has contributed to alleviating these through its development of relevant skills and knowledge, and the confidence and motivation to apply it.

Some participants reported that university policies held them back in commercialising their research, as well as recruitment difficulties and challenges with onboarding people onto their teams.

The process evaluation identified specific areas where alumni/graduates could be further supported:

- Early training in business economics
- Encouragement to put networking skills to use
- Formulation of specific business challenges for the challenge-led cohort

8.2.3 Assess the causal mechanism with respect to the culture and behaviour of academics (e.g., entrepreneurial skills, perceptions of commercialisation, intent to commercialise) and their institutions and the challenges they face. Consider whether the programme is working as intended.

CyberASAP has contributed to the skills, confidence, and knowledge needed to spin-out a company. Beyond that, it has affected the propensity to commercialise, helping academics to embrace a pathway to impact for their research which they may not have considered before.

Evidence for behaviour change comes from the reports of many researchers who attribute their decision to spin-out to the structured CyberASAP support. The specific mechanisms could be due to increased confidence, an explanation of a route to commercialisation that was not previously considered, and the networking and connections to further forms of support and advice which the programme provides to facilitate spin-out formation.

8.2.4 To what extent has the programme been effective in turning research outputs into the marketplace (e.g., spin-out companies, product licensing, and the development of new products and services)?

The programme significantly increases the probability of successful spin-out formation and accelerates the process by providing early-stage commercialisation expertise that many researchers lack. CyberASAP participants have spun out companies, licensed technology, and developed products and services.

There are also examples of further knowledge and IP generation, through registration of patents and provision of outputs in open-source format.

8.2.5 Have there been any additional or unintended benefits of the programme (improved commercial awareness, better inter-university collaboration, improved commercial knowledge of university knowledge exchange teams, private sector investment, patents, licenses, open-source software)?

The programme has led to improved commercial awareness, which has in turn affected how alumni think about their research through a market lens. The survey evidence has reported private sector investment, and dissemination of IP through patents and open-source software.

A key additional benefit has been through licensing. The primary route to commercialisation supported by CyberASAP is spin-out company formation; the number of registered CyberASAP Alumni Companies is a KPI for the programme. However, working with established companies can be efficient (for example, in sectors with high capital costs), and in these cases licensing is an effective route to market. Some CyberASAP projects have licensed their technology instead, and one specifically reported that the skills learned in the programme helped them to refine their product for that model.

8.2.6 Recommendations arising from the impact evaluation

Recommendation 7. CyberASAP should continue to provide comprehensive, high-quality commercialisation training to ensure participants are well-equipped to refine their ideas into commercially viable products and are well-prepared to present to investors.

Recommendation 8. CyberASAP should investigate expert mentoring in niche technology areas such as deep tech to improve the quality of training in these.

Recommendation 9. CyberASAP should implement longer-term support mechanisms to support business survival and growth post-programme participation. The impact on survival rates is hardest to evidence at this point, so support should be forward-looking to head off any problems companies may face, and should be customised for individual sectors, and additional to support provided by universities and their TTOs.

8.3. Value for money evaluation

This section summarises the key findings against the research questions. It includes recommendations that could improve value for money through the "4 'E's" identified by the National Audit Office – making the programme more effective, efficient, economic, or equitable.

8.3.1 To what extent has the program used public resources in a way that maximises public value?

The 4Es assessment suggests that CyberASAP exhibits strong "Good" overall value for money, with particularly strong results in spin-out formation and follow-on investment. It has met its targets on participation and progress while staying within budget, and accelerated progress towards commercialisation. The latter result applies even to academics who thought they might have commercialised even without CyberASAP support.

By its nature, CyberASAP has low deadweight – by focusing on academic researchers, it is stimulating economic activity which is innovative and unlikely to have arisen from other sources. As a result, while economic impacts might take a long time to arise, the resulting products and services are more likely to be truly novel and in the long term could be internationally tradable.

8.3.2 Is this programme the best possible use of public funds to achieve the intended outcomes?

Targets for team participation and progress have been achieved without using the full allocated budget. As set out above the support is likely to be highly additional: it will benefit recipients that might not otherwise have generated commercial activity and produce novel products and services. As such, it is complementary to support aimed at existing businesses.

In real terms (2024/25 prices), every £1 of programme expenditure has generated ~£3.90 of spin-out investment across Cohorts 1–8. This ratio would be expected to rise as later cohorts move toward spin-out formation and investment. We estimate, using survey evidence, that 70% of this is wholly due to CyberASAP (i.e. the other 30% would have occurred anyway). This amounts to £2.73 of wholly additional spin-out investment per £1 programme expenditure in real terms.

CyberASAP spin-outs have created approximately 76 net additional jobs, which are currently responsible for £8.89 million in annual GVA, after accounting for deadweight, displacement, and leakage. The ratio of annual recurring GVA to annual programme cost is currently about 6.32:1. Over time, if spin-out jobs persist and grow, the cumulative economic return will improve accordingly.

8.3.3 How could value for money be or have been improved?

The programme has performed very well in terms of its economy – spending less while maintaining quality. Overall VfM could be improved by redirecting resources:

- The numbers accepted into Phase 1 could be increased, recognising that approx. 50% will drop out between Phase 1A and Phase 2; this could increase the quantity of outputs
- Resources could be proactively directed to additional targeted support for those academic teams which do proceed to later phases, based on their challenges, weaknesses, and needs; this could increase the quality of the business propositions arising from the programme.

8.3.4 Recommendations arising from the value for money evaluation

Recommendation 10. The programme demonstrates good economy through budget management and minimising overheads. However, CyberASAP should improve its effectiveness and efficiency by securing more tailored mentor expertise to support sectors such as deep tech. This would improve quality of outputs by directing bespoke training towards demos and final pitches in niche sectors, which were mentioned as a relative weakness, and could also be deployed towards longer-term support.

Recommendation 11. The current level of underspend per cohort should be investigated – this could be deployed towards the extra support mentioned in recommendation 1, or towards recruiting more academics per cohort if there is demand for this among high-quality applicants.

Recommendation 12. Building on the progress in regional reach and the increase in female principal investigators since Cohort 1, CyberASAP should consolidate its equity gains by systematically recording and reporting the gender and ethnicity of all team members (not just the PI) at each phase-gate, using those data to fine-tune outreach so that improvements are transparent, evidence-led, and firmly linked to the wider talent pipeline.

Appendix A – Evaluation Questions

The evaluation should determine how CyberASAP has performed since it was first launched in 2016. It should assess the implementation of CyberASAP and provide evidence as to the effectiveness and efficiency of the programme by answering the following key questions:

Process Evaluation

- To what extent was the programme delivered as intended?
- What worked well, or less well, for whom and why?
- Were there any unexpected or unintended issues with the delivery of the programme?
- What can be learned from the delivery methods used?
- To what extent did external factors influence the delivery and functioning of the programme?
- How might the existing programme be improved to become more effective?

Effectiveness

- To what extent has the programme been effective at enabling the academic sector to commercialise their ideas or speed up this process? Compare the key performance indicators to the aims of the programme.
- Have the expected outcomes been accomplished within the expected cost?
- What are the challenges facing academics upon graduation of the programme? To what extent has the programme been effective at mitigating these? How else might the programme support alumni/graduates?
- Assess the causal mechanism with respect to the culture and behaviour of academics (e.g., entrepreneurial skills, perceptions of commercialisation, intent to commercialise) and their institutions and the challenges they face. Consider whether the programme is working as intended.
- To what extent has the programme been effective in turning research outputs into the marketplace (e.g., spin-out companies, product licensing, and the development of new products and services)?
- Have there been any additional or unintended benefits of the programme (improved commercial awareness, better inter-university collaboration, improved commercial knowledge of university knowledge exchange teams, private sector investment, patents, licenses, open-source software)?
- To what extent is there a difference between the outcomes of the programme across different types of universities (e.g., post 1992 universities, Russell Group universities and Academic Centres of Excellence in Cyber Security Research (ACE-CSR), different regions? What accounts for any differences?
- What is the programme's impact on the UK economy? Consider the value of the sector and its relevance to economic growth and productivity. Have there been any impacts on local/regional economies?

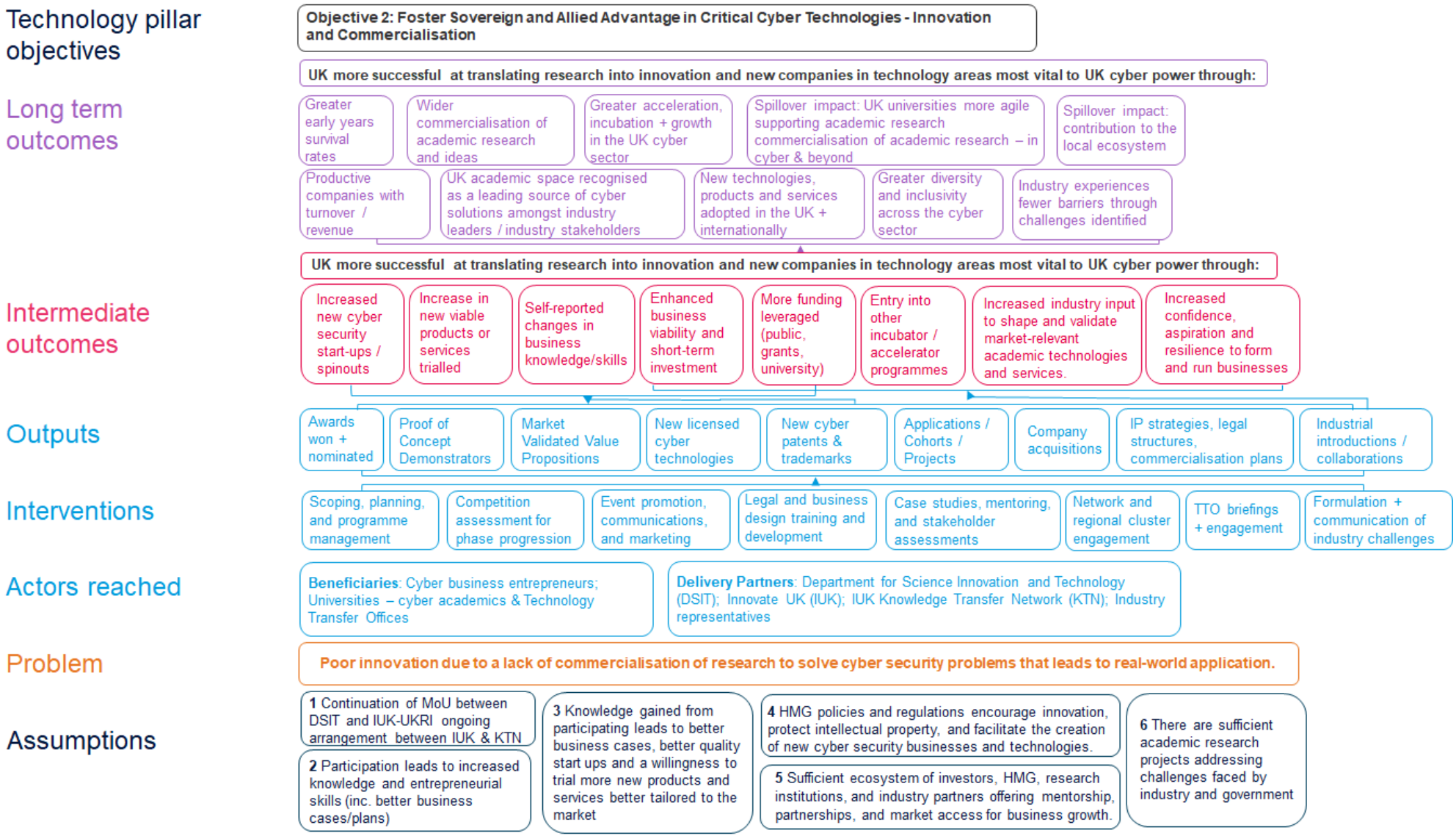
Value for Money

- To what extent has the program used public resources in a way that maximises public value?
- Is this programme the best possible use of public funds to achieve the intended outcomes?[92]
- How could value for money be or have been improved?

[92] The guidance in the Invitation to Tender suggested that this question should look beyond assessing whether the benefits are greater than the costs, and that it would be helpful to measure the cost per output generated.

Appendix B – Theory of Change

Figure 8: CyberASAP ToC



Appendix C – Benchmarking Evidence

A.1. Transition to Practice (TTP) programme

The following table provides a comparison of CyberASAP and the Transition to Practice programme which was funded and delivered by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) in the United States.

Table 42: Transition to Practice (TTP) in the United States

Programme name	CyberASAP – UK	Transition to Practice (TTP) – United States
Funder	Funded by DSIT. CyberASAP was formerly funded by DCMS[93].	Funded by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T)[94].
Delivery partner	Currently cohorts are delivered by Innovate UK, previous cohorts were delivered by Knowledge Transfer Network (KTN)[95].	The TTP programme is delivered by DHS S&T.[96]
Budget	The total budget for CyberASAP is not publicly specified. Projects receive the grant only for the duration they are on the programme. The grant is largely to cover academic salaries, although it can also be used on Phase 2 Proof of Concept development[97].	The TTP programme has leveraged over $250 million in funding from other federal agencies (including Department of Energy National Labs and Federally Funded Research and Development Centres). However, exact TTP budget and the amount of funding allocated to each project/technology is not publicly specified[98].
Delivery timeframe	CyberASAP was launched in 2017 and is still ongoing, with one cohort of researchers each year.	The TTP programme was launched in 2012 and was replaced by an expanded programme called the Commercialisation Accelerator Program (CAP) in 2019. CAP is an expanded version of TTP focusing on all technologies impacting national security such as data analytics, screening, and detection[99].
Programme objectives	CyberASAP is designed to support the achievement of the Technology Advantage Pillar in the UK's National Cyber Strategy 2022, specifically Objective 2: '*Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace*'[100].	The TTP programme has three key objectives: To identify promising technologies that address an existing or imminent cybersecurity need that impacts national security.

[93] CyberASAP - Innovate UK Business Connect (Accessed 30/01/2025).
[94] TTP | Homeland Security (Accessed 30/01/2025).
[95] CyberASAP - Innovate UK Business Connect (Accessed 30/01/2025).
[96] TTP | Homeland Security (Accessed 30/01/2025).
[97] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK (Accessed 31/01/2025).
[98] "DHS S&T Cyber Security Division (CSD) & Silicon Valley Innovation Program" (Accessed 31/01/2025).
[99] CAP Fact Sheet 2020 (Accessed 30/01/2025).
[100] National Cyber Strategy 2022 (HTML) - GOV.UK (Accessed 31/01/2025).

Programme name	CyberASAP – UK	Transition to Practice (TTP) – United States
		To increase utilisation through partnerships, product development efforts and commercialisation. Improve the long-term ability of federal government research organisations to transition technology more efficiently[101].
Programme delivery	CyberASAP supports a cohort of projects annually, with an average of 23 projects per cohort. CyberASAP is delivered in a two-phase approach starting in April each year and lasting 12 months. ▪ Phase 1A: development of Value Proposition (approximately two months and up to £16,000 grant). Phase 1B: Market Validation of Value Proposition (approximately two months and up to £16,000 grant). Projects are then assessed at the end of Phase 1A and 1B by external, industry-led panels and only those projects which pass can proceed to the next stage. Application to Phase 2 is via a closed InnovateUK competition and is invitation only to those who have successfully proceeded onwards from Phase 1B. ▪ Phase 2: Development of Proof of Concept (PoC) (approximately five months and up to £60,000 grant)[102]. Innovate UK / KTN specialists deliver bootcamps, training, mentoring, peer to peer learning, tools, and organise an industry showcase (demonstration day). External mentors provide sessions on sales and presentations, PR, marketing and communications, market validation, investor readiness, IP, and legal issues, and developing a Proof of Concept[103].	The TTP programme supported a cohort of technologies annually. Selected technologies undergo a 36-month process that includes validating the technology through testing, evaluation, and pilot deployments. This process aims to accelerate time-to-market by offering training and market research. Additionally, it connects researchers with investors and potential licensors through outreach, industry events, and Technology Demonstration Days[104]. Every 18-months, the TTP programme hosted an R&D showcase to present the research efforts to public and private partners. The Technology Demonstration Days, held multiple times annually, helped raise awareness of cybersecurity solutions ready for operational use as well as identifying new security requirements which guided the launch of new research focus areas[105].
Number of funded projects	Since 2017, CyberASAP has supported over 170 projects from UK universities to develop their innovations.	The TTP programme supported over 60 technologies between 2012 and 2019. Each year, a cohort of approximately eight technologies were selected.

[101] TTP | Homeland Security (Accessed 30/01/2025).
[102] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK (Accessed 31/01/2025).
[103] CyberASAP_ImpactInsight_Report-1.pdf (Accessed 31/01/2025).
[104] TTP—Transition to Practice Technology Guide (Accessed 30/01/2025).
[105] Cyber Security R&D Program a Launching Pad for New Solutions | Homeland Security (Accessed 30/01/2025).

Programme name	CyberASAP – UK	Transition to Practice (TTP) – United States
		The TTP programme invested in technologies spanning a range of cyber areas, primarily focusing on: ▪ Network security ▪ Threat intelligence and analysis ▪ Industrial and IoT security ▪ Malware detection[106]
Eligibility criteria of funded projects	Applicants must meet the following eligibility requirements: ▪ Based in a UK academic institution. ▪ Have a cybersecurity idea. ▪ Be interested in the commercialisation of their idea. ▪ Have the support of their academic institution's Technology Transfer Office (TTO), or equivalent. CyberASAP offers two funding strands: (1) Industry-challenge-led strand and (2) Open strand. The Industry Challenge – led strand is open for eligible individuals from any UK academic institution who address one of three key industry challenge areas from AI model security, software supply chain security and Industrial Internet of Things (IIOT) or Operation Technology (OT) security. Open strand is open for any eligible individual. The programme does not fund any projects which are defence focused[107].	The TTP programme targets technologies developed through federal R&D that have a high probability of successful transition to the commercial market within three years and are expected to significantly impact cybersecurity. It identifies technologies from various federally funded R&D sources, including: ▪ Department of Energy National Labs ▪ Department of Defense-Affiliated Labs ▪ Federally Funded Research and Development Centers (FFRDC) ▪ University-Affiliated Research Centers (UARC) ▪ Universities receiving federal grants ▪ Examples include Pacific Northwest National Laboratory, MIT Lincoln Lab, and Los Alamos National Laboratory. ▪ Technologies are selected based on their uniqueness of approach and market potential. ▪ TTP targets later-stage R&D that is ready for transition into an operational environment[108].
Intended outcomes and impacts	According to the CyberASAP Theory of Change (ToC), the programme has the following expected intermediate and long-term outcomes: Intermediate outcomes ▪ Increased new cybersecurity start-ups / spinouts. ▪ Increase in new viable products or services trialled.	See programme objectives.

[106] S&T TTP Infographic | Homeland Security (Accessed 30/01/2025).
[107] Competition overview - Cyber security academic startup accelerator programme 2024-25: phase 1 - Innovation Funding Service (Accessed 31/01/2025).
[108] TTP | Homeland Security (Accessed 30/01/2025).

Programme name	CyberASAP – UK	Transition to Practice (TTP) – United States
	▪ Self-reported changes in business knowledge / skills. ▪ Enhanced business viability and short-term investment. ▪ More funding leveraged (public, grants, university). ▪ Entry into other incubator / accelerator programmes. ▪ Increased industry input to shape and validate market-relevant academic technologies and services. ▪ Increased confidence, aspiration, and resilience to form and run businesses. Long-term outcomes ▪ Productive companies with turnover/revenue. ▪ UK academic space recognised as a leading source of cyber solutions amongst industry leaders/industry stakeholders. ▪ New technologies, products and services adopted in the UK and internationally. ▪ Greater diversity and inclusivity across the cyber sector. ▪ Industry experiences fewer barriers through challenges identified. ▪ Greater early year survival rates. ▪ Wider commercialisation of academic research and ideas. ▪ Greater acceleration, incubation, and growth in the UK cyber sector. ▪ Spillover impact: UK universities are more agile supporting commercialisation of academic research in cyber and beyond. ▪ Spillover impact: contribution to the local ecosystem.	
Observed outcomes and impacts	Of the 170 projects supported by CyberASAP, 32 startup companies have been formed. The alumni projects have leveraged £40 million in funder funding from various sources including	Since its inception in 2012, the TTP programme facilitated the launch of seven new startups and successful transition of 21 technologies, five of which were made available as open-source software[112].

[112] CAP Fact Sheet 2020 (Accessed 30/01/2025).

Programme name	CyberASAP – UK	Transition to Practice (TTP) – United States
	private investment, acquisition, VC investment, angel investment and seed funding[109]. Graduates of the programme have joined further (in some cases multiple) accelerator and incubator programmes including HutZero (at least three projects), IoT Accelerator Wales, Cyber101 (at least five projects), MI Garage and Barclaycard Techstars[110]. CyberASAP participants reported developing entrepreneurial skills and confidence because of participation[111].	Examples of the open-source software made available through TTP include: ▪ KeyLime (TPM Based Trust in the Cloud technology) developed by researchers at the Massachusetts Institute of Technology Lincoln Laboratory in 2017. ▪ PcapDB (Optimised Full Packet Capture technology) developed by the Los Alamos National Laboratory in 2017[113]. ▪ Hone (Host and Network Data Correlation technology) developed by the Pacific Northwest National Laboratory in 2015, actively used by Google and others. ▪ SCOT (incident response threat intel technology) developed by the Pacific Northwest National Laboratory in 2015, is in use by the United States government[114]. ▪ LOCKMA is a software component designed to significantly simplify the task of adding cryptographic protections and underlying key management to software applications and embedded devices. In 2012, LOCKMA was recognized by the prestigious R&D 100 award; a realization of LOCKMA as an FPGA core resulted in two USPTO patent applications and won the MIT Lincoln Laboratory Best Invention Award[115]. TTP has ensured that the results of $118 million of federal R&D investment '*doesn't sit on the shelf*'[116].
Successful spinouts - examples	The following startup companies have been formed by CyberASAP participants: ▪ Lupovis (AI-based solution which leads cyber attackers and ransomware away from high value assets) spun out as a startup. Lupovis applied to CyberASAP through the University of Strathclyde as part of the fourth cohort. The company currently has four employees[117]. In 2021, the company secured a pre-seed investment of over €700k. Lupovis' founder,	The TTP programme facilitated the launch of seven new start-ups, including: ▪ ZeroPoint (weaponized Document detection technology) spun off as a startup company called ZeroPoint Dynamics. ZeroPoint was developed by researchers at the University of North Carolina at Chapel Hill and funded by the National Science Foundation. It was the eighth cybersecurity technology transitioning

[109] CyberASAP - Innovate UK Business Connect (Accessed 31/01/2025).
[110] CyberASAP_ImpactInsight_Report-1.pdf (Accessed 31/01/2025).
[111] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK
[113] Snapshot: S&T TTP Program Moved 10 Technologies to Marketplace in FY17 | Homeland Security (Accessed 31/01/2025).
[114] "DHS S&T Cyber Security Division (CSD) & Silicon Valley Innovation Program" (Accessed 31/01/2025).
[115] csd-ttp-technology-guide-volume-2(1).pdf
[116] S&T TTP Infographic | Homeland Security (Accessed 31/01/2025).
[117] Lupovis - Innovate UK Business Connect (Accessed 31/01/2025).

Programme name	CyberASAP – UK	Transition to Practice (TTP) – United States
	Xavier Bellekens, attributes the company's success to CyberASAP saying '*without CyberASAP we wouldn't have a company at all*'[118]. ▪ Cydon (decentralised data management platform technology) spun out as a startup company. Cydon applied to CyberASAP through the University of Wolverhampton and were part of the second cohort of the programme. The company have now filed a patent in the UK and the United States[119]. ▪ Awen Collective spun out as a startup company. Awen Collective applied to CyberASAP through the University of South Wales as part of the first cohort of the programme. The company currently has three employees. They have attracted post-programme funding through equity investment from Development Bank of Wales, Inspire Growth Wales and angels, and investment from SFC Capital and Dutch Security Tech Fund of TIIN Capital[120]. In 2023 Awen Collective was acquired by Sapphire Technologies.[121]	to commercialisation as part of TTP[122]. ZeroPoint Dynamics now has a core team of six employees and continues to offer services to DHS and the Defense Advanced Research Projects Agency[123]. ▪ PEACE (Policy Enforcement and Access Control for Endpoints technology) was developed at the Worcester Polytechnic Institute. The technology, which protects end-point devices by intercepting all new network connections and vetting them at a centralised network controller, was spun out by a Massachusetts-based startup ContexSure Networks, Inc[124]. ▪ FLOWER (Network Flow AnalyzER) was developed by Pacific Northwest National Laboratory and licensed by zSofTech Solutions. FLOWER has been deployed at over 100 US government sites and private corporations to analyse network traffic[125]. It was the tenth cybersecurity technology transitioning to commercialisation as part of TTP[126].

[118] CyberASAP Alumni Insights: "Don't worry about people stealing your idea!" - Innovate UK Business Connect (Accessed 31/01/2025).
[119] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK (Accessed 31/01/2025).
[120] Awen Collective - Innovate UK Business Connect (Accessed 31/01/2025).
[121] About — Awen by Sapphire (Accessed 31/01/2025).
[122] ZeroPoint Earns Mega Points with DHS | AFCEA International (Accessed 31/01/2025).
[123] Zeropoint Dynamics (Accessed 31/01/2025).
[124] Snapshot: S&T TTP Program Moved 10 Technologies to Marketplace in FY17 | Homeland Security (Accessed 31/01/2025).
[125] TTP—Transition to Practice Technology Guide (Accessed: 24/01/2025).
[126] News Release: DHS S&T Licenses New Cybersecurity Tech to Atlanta Small Business | Homeland Security (Accessed 31/01/2025).

A.2. Cybersecurity Innovation Network

The following table provides a comparison of CyberASAP and the Cybersecurity Innovation Network (CSIN) funded by ISED and currently being delivered by the NCC in Canda.

Table 43: Cybersecurity Innovation Network (CSIN) in Canada

Programme name	CyberASAP – UK	Cybersecurity Innovation Network (CSIN) – Canada
Funder	Funded by DSIT. CyberASAP was formerly funded by DCMS[127].	Funded by Innovation, Science and Economic Development Canada (ISED)[128].
Delivery partner	Currently cohorts are delivered by Innovate UK, previous cohorts were delivered by Knowledge Transfer Network (KTN)[129].	CSIN is led by the National Cybersecurity Consortium (NCC)[130].
Budget	The total budget for CyberASAP is not publicly specified. Projects receive the grant only for the duration they are on the programme. The grant is largely to cover academic salaries, although it can also be used on Phase 2 Proof of Concept development[131].	Investment from ISED of CAD 80 million across four years (2021-22 to 2024-25). Funded projects must provide a 1:1 cost-matching of the CAD 80 million investment meaning the programme is expected to result in a total minimum investment of CAD 160 million over four years. Eligible project costs could include: ▪ Recruiting and retaining faculty, students, researchers, support engineers and admin staff. ▪ Direct research costs e.g. facility access, equipment, materials, salaries, and stipends. ▪ Costs for knowledge mobilisation, technology exchange, and exploitation (e.g., prototype development, IP). ▪ Up to 20% of funds may be used for equipment and infrastructure for research development and training[132].
Delivery timeframe	CyberASAP was launched in 2017 and is still ongoing, with one cohort of researchers each year.	CSIN is being delivered across four years (2021-22 to 2024-25)[133].
Programme objectives	CyberASAP is designed to support the achievement of the Technology Advantage Pillar in the UK's National Cyber Strategy 2022,	CSIN has three key objectives:

[127] CyberASAP - Innovate UK Business Connect (Accessed 30/01/2025).
[128] Program_guide-Cyber_Security_Innovation_Network.pdf (Accessed 30/01/2025).
[129] CyberASAP - Innovate UK Business Connect (Accessed 30/01/2025).
[130] The Government of Canada has Appointed the NCC to Lead the Cybersecurity Innovation Network | National Cybersecurity Consortium (Accessed 30/01/2025).
[131] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK (Accessed 31/01/2025).
[132] Program_guide-Cyber_Security_Innovation_Network.pdf (Accessed 30/01/2025).
[133] Program_guide-Cyber_Security_Innovation_Network.pdf (Accessed 30/01/2025).

Programme name	CyberASAP – UK	Cybersecurity Innovation Network (CSIN) – Canada
	specifically Objective 2: '*Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace*'[134].	▪ To support R&D in cybersecurity through encouraging collaboration between Canada's post-secondary institutions (PSIs), the private sector, and other partners to accelerate the development of innovative cyber security products and services. ▪ To accelerate the commercialisation of cybersecurity products, services and processes that enter the marketplace. ▪ To grow and diversify Canada's cybersecurity talent pipeline by recruiting and retaining faculty and trainers. Also to enhance curriculum development, training, and skill-building through industry partnerships[135].
Programme delivery	CyberASAP supports a cohort of projects annually, with an average of 23 projects per cohort. CyberASAP is delivered in a two-phase approach starting in April each year and lasting 12 months. ▪ Phase 1A: development of Value Proposition (approximately two months and up to £16,000 grant). Phase 1B: Market Validation of Value Proposition (approximately two months and up to £16,000 grant). Projects are then assessed at the end of Phase 1A and 1B by external, industry-led panels and only those projects which pass can proceed to the next stage. Application to Phase 2 is via a closed InnovateUK competition and is invitation only to those who have successfully proceeded onwards from Phase 1B. ▪ Phase 2: Development of Proof of Concept (PoC) (approximately five months and up to £60,000 grant)[136]. Innovate UK / KTN specialists deliver bootcamps, training, mentoring, peer to peer learning, tools, and organise an industry showcase (demonstration day).	CSIN has committed funding for projects ranging from CAD 79,500 to CAD 2 million, with an average of CAD 607,721. They hold annual Calls for Proposals, with Calls for Proposals held in 2023 and 2024, and plans for another in 2025[138]. Eligible activities include: ▪ R&D and commercialisation: including conceptual design validation, Proof of Concept, prototype development, IP creation, product testing and new product/services development. ▪ Commercialisation: business development services for firms to access to new customers and expand markets (e.g. market studies, advisory services, pitch days) and activities relating to the exploitation and retention of IP. ▪ Skills development: addressing skills gaps, offering training modules, developing education pathways, supporting curriculum development, coaching/mentoring, and work-integrated learning opportunities. The lead recipient is responsible for coordinating and overseeing these activities,

[134] National Cyber Strategy 2022 (HTML) - GOV.UK (Accessed 31/01/2025).
[135] Program_guide-Cyber_Security_Innovation_Network.pdf (Accessed 30/01/2025).
[136] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK (Accessed 31/01/2025).
[138] Funded Projects | National Cybersecurity Consortium (Accessed 30/01/2025).

Programme name	CyberASAP – UK	Cybersecurity Innovation Network (CSIN) – Canada
	External mentors provide sessions on sales and presentations, PR, marketing and communications, market validation, investor readiness, IP, and legal issues, and developing a Proof of Concept[137].	including organising network events, conferences, and managing network offices[139].
Number of funded projects	Since 2017, CyberASAP has supported over 170 projects from UK universities to develop their innovations.	CSIN has funded 56 projects across two annual Calls for Proposals (in 2023 and 2024), split as follows: ▪ R&D: 39 projects (CAD 18.7 million). ▪ Commercialisation: four projects (CAD 3.9 million). ▪ Training: 13 projects (CAD 11.4 million)[140].
Eligibility criteria of funded projects	Applicants must meet the following eligibility requirements: ▪ Based in a UK academic institution. ▪ Have a cybersecurity idea. ▪ Be interested in the commercialisation of their idea. ▪ Have the support of their academic institution's Technology Transfer Office (TTO), or equivalent. CyberASAP offers two funding strands: (1) Industry-challenge-led strand and (2) Open strand. The Industry Challenge – led strand is open for eligible individuals from any UK academic institution who address one of three key industry challenge areas from AI model security, software supply chain security and Industrial Internet of Things (IIOT) or Operation Technology (OT) security. Open strand is open for any eligible individual. The programme does not fund any projects which are defence focused[141].	Applicants must be comprised as a network led by three or more Canadian centres of expertise on cybersecurity affiliated with PSIs and must be federally incorporated as a not-for-profit organisation. Applicants must be representative of the diversity of Canada's cyber security ecosystem with the following expected to be included in the network: centres of expertise on cybersecurity affiliated with PSIs, private sector, Canadian PSIs, not-for-profit organisations, and provincial/territorial/municipal governments. Applicants must be pan-Canadian, i.e. with centres of expertise on cybersecurity from across Canada's regions. Applicants must commit to match the funds requested of CSIN.
Intended outcomes and impacts	According to the CyberASAP Theory of Change (ToC), the programme has the following expected intermediate and long-term outcomes: Intermediate outcomes	Medium-term outcomes and associated performance indicators (2023/24 to 2024/25): ▪ R&D: Increased collaboration between industry and academia.

[137] CyberASAP_ImpactInsight_Report-1.pdf (Accessed 31/01/2025).
[139] Program_guide-Cyber_Security_Innovation_Network.pdf (Accessed 30/01/2025).
[140] Funded Projects | National Cybersecurity Consortium (Accessed 30/01/2025).
[141] Competition overview - Cyber security academic startup accelerator programme 2024-25: phase 1 - Innovation Funding Service (Accessed 31/01/2025).

Programme name	CyberASAP – UK	Cybersecurity Innovation Network (CSIN) – Canada
	▪ Increased new cybersecurity start-ups / spinouts. ▪ Increase in new viable products or services trialled. ▪ Self-reported changes in business knowledge / skills. ▪ Enhanced business viability and short-term investment. ▪ More funding leveraged (public, grants, university). ▪ Entry into other incubator / accelerator programmes. ▪ Increased industry input to shape and validate market-relevant academic technologies and services. ▪ Increased confidence, aspiration, and resilience to form and run businesses. Long-term outcomes ▪ Productive companies with turnover/revenue. ▪ UK academic space recognised as a leading source of cyber solutions amongst industry leaders/industry stakeholders. ▪ New technologies, products and services adopted in the UK and internationally. ▪ Greater diversity and inclusivity across the cyber sector. ▪ Industry experiences fewer barriers through challenges identified. ▪ Greater early year survival rates. ▪ Wider commercialisation of academic research and ideas. ▪ Greater acceleration, incubation, and growth in the UK cyber sector. ▪ Spillover impact: UK universities are more agile supporting commercialisation of academic research in cyber and beyond. ▪ Spillover impact: contribution to the local ecosystem.	▪ Number of collaborative R&D projects involving both industry and academic participants. ▪ Commercialisation: Network projects advance product and knowledge development towards commercialisation ▪ Number of projects that advance over a minimum of two TRLs. ▪ Number of patents filed and/or granted because of network activities. ▪ Skills and talent development: Increased opportunities for students and cyber security workers to develop cyber security related skills and knowledge. ▪ Number of new post-secondary students participating in cyber security training activities. ▪ Number of participants from underrepresented groups engaged in cyber security skills development activities through the network. ▪ Number of workers in cyber-related fields participating in cyber security training, reskilling, and upskilling activities established by the network. ▪ Number of post-secondary students participating in co-op and/or work-integrated learning programs established by the network. Long-term outcomes and performance indicators (2025/26 to 2026/27 and onwards): ▪ Commercialisation: Canadian businesses commercialise new or improved cyber security innovation. ▪ Value of sales of cyber security products and services. ▪ Skills and talent development: Industry can access qualified and skilled cyber security pipeline. ▪ Number of people holding credentials in cyber security. ▪ Number of graduates of academic programs and trainees entering the cyber security workforce.

Programme name	CyberASAP – UK	Cybersecurity Innovation Network (CSIN) – Canada
		▪ Percentage of cyber security professionals from underrepresented groups entering the workforce. ▪ Percentage of firms participating in the network indicating recent graduates of academic programs and trainees entering the workforce meet industry needs[142].
Observed outcomes and impacts	Of the 170 projects supported by CyberASAP, 32 startup companies have been formed. The alumni projects have leveraged £40 million in funder funding from various sources including private investment, acquisition, VC investment, angel investment and seed funding[143]. Graduates of the programme have joined further (in some cases multiple) accelerator and incubator programmes including HutZero (at least three projects), IoT Accelerator Wales, Cyber101 (at least five projects), MI Garage and Barclaycard Techstars[144]. CyberASAP participants reported developing entrepreneurial skills and confidence because of participation[145].	No observed outcomes to include yet, intend to include from discussion with CSIN / NCC contacts via email or interview.
Successful spinouts - examples	The following startup companies have been formed by CyberASAP participants: ▪ Lupovis (AI-based solution which leads cyber attackers and ransomware away from high value assets) spun out as a startup. Lupovis applied to CyberASAP through the University of Strathclyde as part of the fourth cohort. The company currently has four employees.[146] In 2021, the company secured a pre-seed investment of over €700k. Lupovis' founder, Xavier Bellekens, attributes the company's success to CyberASAP saying '*without CyberASAP we wouldn't have a company at all*'[147]. ▪ Cydon (decentralised data management platform technology) spun out as a startup company. Cydon applied to CyberASAP through the University of Wolverhampton	No successful spinouts to date.

[142] Program_guide-Cyber_Security_Innovation_Network.pdf (Accessed 30/01/2025).
[143] CyberASAP - Innovate UK Business Connect (Accessed 31/01/2025).
[144] CyberASAP_ImpactInsight_Report-1.pdf (Accessed 31/01/2025).
[145] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK
[146] Lupovis - Innovate UK Business Connect (Accessed 31/01/2025).
[147] CyberASAP Alumni Insights: "Don't worry about people stealing your idea!" - Innovate UK Business Connect (Accessed 31/01/2025).

Programme name	CyberASAP – UK	Cybersecurity Innovation Network (CSIN) – Canada
	and were part of the second cohort of the programme. The company have now filed a patent in the UK and the United States[148]. Awen Collective spun out as a startup company. Awen Collective applied to CyberASAP through the University of South Wales as part of the first cohort of the programme. The company currently has three employees. They have attracted post-programme funding through equity investment from Development Bank of Wales, Inspire Growth Wales and angels, and investment from SFC Capital and Dutch Security Tech Fund of TIIN Capital[149]. In 2023 Awen Collective was acquired by Sapphire Technologies[150].	

[148] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK (Accessed 31/01/2025).
[149] Awen Collective - Innovate UK Business Connect (Accessed 31/01/2025).
[150] About — Awen by Sapphire (Accessed 31/01/2025).

A.3. ON Innovation Program

The following table provides a comparison of CyberASAP and CSIRO's ON Innovation Program (ON Program) delivered in Australia. The ON Program comprises two sub-programmes:

- **ON Prime** is the pre-accelerator program which encourages researchers to 'get out of the building' and talk to prospective customers and industry about how their science or technology might address a key challenge for them
- **ON Accelerate** is a commercialisation acceleration programme for entrepreneurial researchers who are ready to translate their idea into a research-driven company. ON Prime can be considered as a precursor to participation in the ON Accelerate programme.

The ON Program was initially delivered from 2015 to 2019. After a three-year hiatus, it was relaunched in 2022. Given the limited timeframe of the second phase (from 2022 onwards), we will primarily focus on the outcomes and impacts achieved during the first phase (2015-2019), as these have been more extensively reported.

Table 44: The ON Program in Australia

Programme name	CyberASAP – UK	ON Innovation Program (ON Program) – Australia
Funder	Funded by DSIT. CyberASAP was formerly funded by DCMS[151].	The On Program is funded by the Commonwealth Scientific and Industrial Research Organisation (CSIRO)[152].
Delivery partner	Currently cohorts are delivered by Innovate UK, previous cohorts were delivered by Knowledge Transfer Network (KTN)[153].	The ON Program is delivered by CSIRO[154].
Budget	The total budget for CyberASAP is not publicly specified. Projects receive the grant only for the duration they are on the programme. The grant is largely to cover academic salaries, although it can also be used on Phase 2 Proof of Concept development[155].	The first phase of delivery was a AUD 20 million funding package delivered over four years from 2015 to 2019[156]. For the second phase of delivery, CSIRO will receive AUD 37.4 million over four years to deliver the ON Program[157].
Delivery timeframe	CyberASAP was launched in 2017 and is still ongoing, with one cohort of researchers each year.	CSIRO originally launched its ON Program in July 2015 as part of its Strategy 2020. The programme was shut down in late 2019. In 2022, three years after its closure, CSIRO revived the programme, which will continue to run until 2026.[158]

[151] CyberASAP - Innovate UK Business Connect (Accessed 30/01/2025).
[152] It's ON: Innovation Program for Researchers - CSIRO (Accessed 03/02/2025).
[153] CyberASAP - Innovate UK Business Connect (Accessed 30/01/2025).
[154] It's ON: Innovation Program for Researchers - CSIRO (Accessed 03/02/2025).
[155] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK (Accessed 31/01/2025).
[156] CSIRO to shutter ON startup program (Accessed 03/02/2025).
[157] 2022-23 Federal Budget - CSIRO (Accessed 03/02/2025).
[158] CSIRO revives its ON Accelerate program - Startup Daily (Accessed 03/02/2025).

Programme name	CyberASAP – UK	ON Innovation Program (ON Program) – Australia
Programme objectives	CyberASAP is designed to support the achievement of the Technology Advantage Pillar in the UK's National Cyber Strategy 2022, specifically Objective 2: '*Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace*'[159].	The ON Program exists to help researchers translate their research to impact, providing the skills and confidence needed to understand and achieve the full potential of their research[160].
Programme delivery	CyberASAP supports a cohort of projects annually, with an average of 23 projects per cohort. CyberASAP is delivered in a two-phase approach starting in April each year and lasting 12 months. ▪ Phase 1A: development of Value Proposition (approximately two months and up to £16,000 grant). Phase 1B: Market Validation of Value Proposition (approximately two months and up to £16,000 grant). Projects are then assessed at the end of Phase 1A and 1B by external, industry-led panels and only those projects which pass can proceed to the next stage. Application to Phase 2 is via a closed InnovateUK competition and is invitation only to those who have successfully proceeded onwards from Phase 1B. ▪ Phase 2: Development of Proof of Concept (PoC) (approximately five months and up to £60,000 grant)[161]. Innovate UK / KTN specialists deliver bootcamps, training, mentoring, peer to peer learning, tools, and organise an industry showcase (demonstration day). External mentors provide sessions on sales and presentations, PR, marketing and communications, market validation, investor readiness, IP, and legal issues, and developing a Proof of Concept[162].	ON Prime is designed to help research teams understand the target audience for their research and improve their skills to communicate their research to them. It is delivered over six days within a nine-week period through a hybrid of in-person and virtual delivery. Teams receive coaching and one-to-one guidance from an assigned innovation mentor. At the end of the programme, there is a showcase event where teams present their progress and network. Additionally, teams can receive up to AUD 5,000 to reward their engagement and learning velocity. ON Accelerate begins with a two-day selection bootcamp, where up to 20 teams are selected from online applications. This bootcamp is an opportunity for teams to demonstrate product-market fit, customer interest and team strength, with input from a network of investors from the Australian deep tech venture capital community. Following this, the immersion week supports teams in increasing their entrepreneurial knowledge, developing skills, progressing their initiatives, and networking with peers, mentors, and startup experts. The top teams are then invited to participate in the full three-month programme. Over the next three months, teams engage with facilitators, other teams, domain coaches, investors, and mentors. The programme concludes with a showcase event where teams present their work to the wider ecosystem and pitch to investors. Teams can also access

[159] National Cyber Strategy 2022 (HTML) - GOV.UK (Accessed 31/01/2025).
[160] It's ON: Innovation Program for Researchers - CSIRO (Accessed 03/02/2025).
[161] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK (Accessed 31/01/2025).
[162] CyberASAP_ImpactInsight_Report-1.pdf (Accessed 31/01/2025).

Programme name	CyberASAP – UK	ON Innovation Program (ON Program) – Australia
		ongoing coaching for up to six months post-programme. ON Accelerate offers teams performance-based payments of up to AUD 80,000 per team. This includes: AUD 20,000 per team provided to TTOs at the beginning of the programme to support specialists such as an interim CEO, CFO etc. Up to AUD 10,000 for goals achieved in-programme. A portion of a AUD 100,000 pool shared across all teams who achieve stretch targets approved by programme facilitators (maximum AUD 50,000 per team)[163].
Number of funded projects	Since 2017, CyberASAP has supported over 170 projects from UK universities to develop their innovations.	It is anticipated that around 100 teams each year between 2022 and 2026 will access the ON Prime programme, with some progressing to the ON Accelerate programme[164]. To date, the programme has had 16 cohorts of ON Prime teams, and eight cohorts of ON Accelerate teams[165].
Eligibility criteria of funded projects	Applicants must meet the following eligibility requirements: ▪ Based in a UK academic institution. ▪ Have a cybersecurity idea. ▪ Be interested in the commercialisation of their idea. ▪ Have the support of their academic institution's Technology Transfer Office (TTO), or equivalent. CyberASAP offers two funding strands: (1) Industry-challenge-led strand and (2) Open strand. The Industry Challenge – led strand is open for eligible individuals from any UK academic institution who address one of three key industry challenge areas from AI model security, software supply chain security and Industrial Internet of Things (IIOT) or Operation	Teams applying to ON Prime must meet the following criteria: ▪ Consist of a team of between two and five participants. ▪ Include one person who is a researcher at an Australian university or Publicly Funded Research Organisation (PFRO)[167]. ▪ Teams applying to ON Accelerate must meet the following criteria: ▪ Consist of a team of between three and six participants. ▪ Include one person who is a researcher at an Australian university or PFRO and a current or recent PhD student from an Australian university or PRFO. ▪ Bringing diverse experience and expertise (e.g. representation from: other Australian

[163] ON Accelerate - CSIRO (Accessed 03/02/2025).
[164] 2022-23 Federal Budget - CSIRO (Accessed 03/02/2025).
[165] ON Program Alumni – Australia's national science and technology accelerator program (Accessed 03/02/2025).
[167] ON Prime - CSIRO (Accessed 03/02/2025).

Programme name	CyberASAP – UK	ON Innovation Program (ON Program) – Australia
	Technology (OT) security. Open strand is open for any eligible individual. The programme does not fund any projects which are defence focused[166].	universities or PFROs, community representatives, industry partners etc[168].
Intended outcomes and impacts	According to the CyberASAP Theory of Change (ToC), the programme has the following expected intermediate and long-term outcomes: Intermediate outcomes ▪ Increased new cybersecurity start-ups / spinouts. ▪ Increase in new viable products or services trialled. ▪ Self-reported changes in business knowledge / skills. ▪ Enhanced business viability and short-term investment. ▪ More funding leveraged (public, grants, university). ▪ Entry into other incubator / accelerator programmes. ▪ Increased industry input to shape and validate market-relevant academic technologies and services. ▪ Increased confidence, aspiration, and resilience to form and run businesses. Long-term outcomes ▪ Productive companies with turnover/revenue. ▪ UK academic space recognised as a leading source of cyber solutions amongst industry leaders/industry stakeholders. ▪ New technologies, products and services adopted in the UK and internationally. ▪ Greater diversity and inclusivity across the cyber sector.	ON Prime – expected outcomes: ▪ Attracting new funding sources. ▪ Establishing new partnerships. ▪ Increasing industry engagement. ▪ Improving clarity around the impact and focus of their research. ▪ Increasing confidence communicating their research. ▪ Forming team bonds in a new project group. ▪ Licensing IP or creating a new startup venture[169]. ON Accelerate – expected outcomes: ▪ Equip, empower, and energise teams to tackle the commercialisation journey. ▪ Support the whole team to develop entrepreneurial skills including networking, pitching and investor engagement. ▪ Assist teams with identifying their customer and the specific problem that they are solving. ▪ Build and validate investment ready, innovative, sustainable, and scalable business models. ▪ Introduce teams to venture funding opportunities, helping them develop a network of experts, investors and supporters and preparing them to succeed[170].

[166] Competition overview - Cyber security academic startup accelerator programme 2024-25: phase 1 - Innovation Funding Service (Accessed 31/01/2025).
[168] ON Accelerate - CSIRO (Accessed 03/02/2025).
[169] ON Prime - CSIRO (Accessed 03/02/2025).
[170] ON Accelerate - CSIRO (Accessed 03/02/2025).

Programme name	CyberASAP – UK	ON Innovation Program (ON Program) – Australia
	▪ Industry experiences fewer barriers through challenges identified. ▪ Greater early year survival rates. ▪ Wider commercialisation of academic research and ideas. ▪ Greater acceleration, incubation, and growth in the UK cyber sector. ▪ Spillover impact: UK universities are more agile supporting commercialisation of academic research in cyber and beyond. Spillover impact: contribution to the local ecosystem.	
Observed outcomes and impacts	Of the 170 projects supported by CyberASAP, 32 startup companies have been formed. The alumni projects have leveraged £40 million in funder funding from various sources including private investment, acquisition, VC investment, angel investment and seed funding[171]. Graduates of the programme have joined further (in some cases multiple) accelerator and incubator programmes including HutZero (at least three projects), IoT Accelerator Wales, Cyber101 (at least five projects), MI Garage and Barclaycard Techstars[172]. CyberASAP participants reported developing entrepreneurial skills and confidence because of participation[173].	During the first phase of the programme from 2016-2019: ▪ The programme has partnered with 40 local universities and research institutes and trained more than 1440 researchers in addition to the 600 CSIRO staff that have been through the program. ▪ CSIRO says it has a '*commercial conversion rate*' of 55% – whereby an idea is turned into a startup company – and that its ON program participants had raised AUD 36.4 million in private capital [174]. ▪ The ON Program participants had also attracted more than AUD 32.8 million in further government grants. The final programs will present their new products and ideas at a final Demo Day on May 7 next year. Since its inception in 2015, the ON Program has: ▪ Supported the creation of over 70 companies. ▪ Created over 700 jobs. ▪ AUD 320 million in commercialisation grants attracted by ON participants.

[171] CyberASAP - Innovate UK Business Connect (Accessed 31/01/2025).
[172] CyberASAP_ImpactInsight_Report-1.pdf (Accessed 31/01/2025).
[173] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK
[174] CSIRO to shutter ON startup program

Programme name	CyberASAP – UK	ON Innovation Program (ON Program) – Australia
		▪ Created a community within the innovation ecosystem of researchers, founders, industry experts, advisors, and investors[175]. Although ON Program does not specifically focus on cybersecurity-related outcomes, many of the projects supported are focused on cybersecurity and related subject areas. Since ON Accelerate's inception it has created 70 new companies and secured more than AUD 305M in commercialisation grants.[176]
Successful spinouts - examples	The following startup companies have been formed by CyberASAP participants: ▪ Lupovis (AI-based solution which leads cyber attackers and ransomware away from high value assets) spun out as a startup. Lupovis applied to CyberASAP through the University of Strathclyde as part of the fourth cohort. The company currently has four employees[177]. In 2021, the company secured a pre-seed investment of over €700k. Lupovis' founder, Xavier Bellekens, attributes the company's success to CyberASAP saying '*without CyberASAP we wouldn't have a company at all*'[178]. ▪ Cydon (decentralised data management platform technology) spun out as a startup company. Cydon applied to CyberASAP through the University of Wolverhampton and were part of the second cohort of the programme. The company have now filed a patent in the UK and the United States.[179] ▪ Awen Collective spun out as a startup company. Awen Collective applied to CyberASAP through the University of South Wales as part of the first cohort of the programme. The company currently has three employees. They have attracted post-programme funding through equity investment from Development Bank of	The following ON program teams have produced successful spinout companies: ▪ Medivox is an AI-powered digital platform that delivers reliable and accessible interpretation tailored for healthcare settings. Cybersecurity and data protection is a core functionality of the tool. The team behind Medivox participated in Cohort 15 of ON Prime (in April – July 2024)[182]. ▪ In January 2025, Medivox was a successful recipient of a ~£100,000 grant from the Cook Government's Innovation Solutions – Digital Health funding programme[183]. ▪ Some notable graduates from the ON program include Emesent (raised AUD 2.5m), Ynomia (raised AUD 3.6m), RapidAIM (raised AUD 1.25m) and Presagen (raised AUD 4.5m)[184]. ▪ WhalePOD - Successful spin out from ON Accelerate 7. After receiving AUD 100k grant in 2020 and AUD 1 million grant in 2021 to develop a proof-of-concept device, WhalePOD took part in ON Accelerate 7 in February 2023. Award: Aqeel Akber, project lead of WhalePOD received the Stanford Australia Foundation CSIRO ON Accelerate 7 Scholarship in May 2023[185].

[175] ON Program Alumni – Australia's national science and technology accelerator program (Accessed 03/02/2025).
[176] Meet the Canberra CSIRO ON Accelerate teams - ErythroSight
[177] Lupovis - Innovate UK Business Connect (Accessed 31/01/2025).
[178] CyberASAP Alumni Insights: "Don't worry about people stealing your idea!" - Innovate UK Business Connect (Accessed 31/01/2025).
[179] Evaluation of the Cyber Security Academic Startup Accelerator - GOV.UK (Accessed 31/01/2025).
[182] ON Alumni – CSIROpedia (Accessed 03/02/2025).
[183] New funding backs local researchers to harness AI in healthcare | Western Australian Government (Accessed 03/02/2025).
[184] CSIRO to shutter ON startup program
[185] WhalePOD

Programme name	CyberASAP – UK	ON Innovation Program (ON Program) – Australia
	Wales, Inspire Growth Wales and angels, and investment from SFC Capital and Dutch Security Tech Fund of TIIN Capital[180]. In 2023 Awen Collective was acquired by Sapphire Technologies[181].	

[180] Awen Collective - Innovate UK Business Connect (Accessed 31/01/2025).
[181] About — Awen by Sapphire (Accessed 31/01/2025).

Appendix D – Case Studies

Case Study 1 – SAIVV

About SAIVV

The SAIVV project focuses on the security of AI models, addressing the need to protect these models against targeted attacks and data leakages with the aim of creating a platform that allows companies to deploy and test their AI models for security vulnerabilities. The team – which formed the project at Sunderland University – participated in Phase 1a and 1b of Year 8 of the programme.

Context and challenges faced

Prior to involvement in the programme, the team had started to explore potential avenues for commercialisation having worked on the project for an extended period. However, they had been facing challenges in finding an existing incubator that would work for them, as many incubators are limited in providing guidance to academics in supporting the transition to a startup/commercial mindset.

'*[Many incubators] are limited in terms of guiding academics who have been in academia for a while in order to make the transition towards having the startup [and] entrepreneurial mindset, especially around how to how to balance between your role as a researcher versus the role as a founder.*'

The team hoped that – through participation in CyberASAP – they would be able to access this commercial support whilst also receiving guidance in the transition from academia to industry as they were aware that the programme approached the incubator model from a more academic perspective. The team hoped there would be many like-minded people within the programme and that the topics covered would be tailored to projects such as SAIVV.

Support received from CyberASAP

The team received a lot of support on commercialisation within the programme, attending a 3-day bootcamp focused on key commercial concepts such as IP, the project's unique selling points, and the fundamentals of developing a startup as academics. In addition to the bootcamp, the team had periodic meetings with their assigned mentor to discuss recent progress and challenges faced, which kept them 'accountable' and 'identify any blind spots' they may have missed.

The team also received considerable support around market validation, as their academic focus prior to the programme had limited awareness of whether the research aligned with the needs of the market. The programme helped develop their understanding of how to approach market validation and product validation, including getting market feedback on their prototype.

The team attended several networking sessions through the programme, leading to them engaging with venture capitalists and investors. This process was viewed positively by the team as it allowed them to gain insight and perspectives from investors which helped to identify how the project could develop moving forward.

'*A number of venture capitalists were invited to network with us and we managed to talk to some of them, listen to their insights and ask some questions around their perspectives around investing in a technical startup and what their concerns slash reservations [may have been].*'

How CyberASAP could be improved

Though the team felt that involvement in CyberASAP was broadly positive, they noted that a greater focus on calculating costs of the startup/commercialisation approach would benefit those transitioning

from academia to industry. Topics such as costs related to IP and monetising hours spent on the project were not covered in great depth, and they would have benefited from crash courses in these areas to enhance understanding. The team felt this could be built in as part of Phase 1B of the programme moving forward, forming a strong foundation of understanding from which to build.

'*So, you've got the idea, you've got the timeline, it's all well and good, but how do you go about calculating the cost of your IP… how do you convert those hours into monetary terms… It would be great if we have a bit of a quick crash course around those areas.*'

The team also noted potential to increase the involvement of university Technology Transfer Offices (TTOs) in the programme to receive their feedback on key university-relevant elements such as IP policy, as each university has different methods of dealing with IP challenges.

Impact and benefits of support received

The team experienced several benefits from involvement in the programme, largely around mindset development. Involvement allowed for a shift in perspective from research-focused to more commercially aware. The team is now more focused on elements such as innovation and product development, whereas before they were far more focused on publishing research. Though the team is no longer involved in the programme, the tools developed through involvement will continue to be applied to future stages of the commercialisation journey, with a focus on market validation and other key areas now very much at the forefront of their thinking.

'*I understood the importance of doing market validation and product validation, but it was more like an afterthought in my mind at that time. But after embarking on the programme I understood that it has to be at the forefront of any entrepreneurial journey.*'

The team has produced a proof of concept following involvement in the programme, with the hope of releasing into the market to collect feedback and validation. Additionally, through CyberASAP, connections have been developed with several regional cyber security clusters in the UK which have supported product and market validation efforts by enabling engagement with relevant industry contacts. This increased engagement with regional clusters has also contributed to increased awareness raising for the team's university (University of Sunderland) across the North East and North West of the UK via the dissemination of an article covering SAIVV throughout these regional clusters and increased engagement with industry.

Lessons learnt from CyberASAP and wider support accessed

Through involvement in CyberASAP, the team has discovered the importance of market validation and the need to begin the validation process as early as possible once you have a functioning product and now place higher value on the importance of understanding your unique selling point / innovative aspects of the product being developed. This mindset change will continue to be applied to the ongoing development of SAIVV as a product, with next steps for the team including the release the proof of concept across industry and exploration of venture funding and other forms of potential investment.

Case Study 2 – CyGamBit

About CyGamBIT

CyGamBIT is a game-based learning solution designed to address online threats faced by young people aged eight to 16. The platform integrates engaging game elements with the latest cybersecurity content to create an interactive and responsive learning experience. It aims to embed learning in a way that is adaptable to the ever-changing digital landscape, ensuring that the content remains relevant and up-to-date.

The project originated from researchers at Bournemouth University, initially focusing on older people. Leveraging their experience working with trading standards, the team developed educational tools such as board games to communicate the risks of financial fraud and scamming, collaborating with organisations like Age UK. However, recognising the need for a more dynamic and adaptable solution, they pivoted to digital game-based learning, shifting their focus to younger audiences. The team participated in Year 6 (Phase 1 and 2) of CyberASAP.

This work led to the creation of Cyber Innovations Ltd., which was founded to develop innovative, evidence-based cybersecurity training solutions. While Cyber First Aid (CFA) is the company's flagship product, CyGamBIT remains a key part of its broader mission to enhance cybersecurity awareness and resilience.

Context and Challenges

CyGamBIT's participation in CyberASAP was driven by the team's desire to transition from an academic focus to a commercially viable model. They recognised the need for the product however faced a lack of market availability, as schools lacked the resources to purchase digital solutions beyond core curriculum requirements.

'Our original idea, just was not commercial, it was academic and that was the problem.'

In addition, the project lead had encountered institutional barriers, as the university department they were part of was not highly supportive of commercialisation efforts. Frequent leadership changes further complicated their ability to secure internal backing. As a result, the project lead moved disciplines to a science and technology department, where leadership was more receptive to initiatives like CyberASAP.

This shift enabled the team to refine Cyber First Aid as the company's primary commercial offering, while continuing to develop CyGamBIT as an engaging tool for younger audiences. CyberASAP provided critical support in shaping Cyber Innovations Ltd. into a sustainable business, ensuring that both CFA and CyGamBIT could be effectively positioned to address different cybersecurity education needs.

Support received from CyberASAP

It was suggested CyberASAP played a crucial role in CyGamBIT's development by providing guidance, mentorship, and resources. The ongoing support from programme mentors and events helped the team navigate challenges through and refine their project. They noted this emotional support from mentors helped them stay motivated and resilient.

'The ongoing support from CyberASAP has been invaluable as sounding boards.'

Workshops and conferences were instrumental in developing transferable skills, such as legal and intellectual property (IP) guidance, which provided critical information for commercialisation. Networking opportunities and alumni support were the most highly valued aspects of the programme. as these interactions broadened their exposure to diverse expertise and perspectives.

'The relationship-building aspect is crucial. It encourages more cross-university working than I could have conceived.'

The structured training offered by CyberASAP was also beneficial, with the project lead advocating for similar funding grants to incorporate training programmes, such as those offered by CyberASAP. This, alongside other core training components (e.g. presentation skills and market validation training), have been critical in the project's development.

'The training programme was crucial, and now I believe all funding grants should come with such a programme for development. Without it, none of this would have happened.'

The project lead found the application process to be efficient and easy to complete, contrasting the programme with other funding streams that often had complex, time-consuming application processes.

How CyberASAP could be improved

While the alumni network was highly beneficial, the team suggested that more informal alumni interactions earlier in the process would have been helpful. They noted that many formal alumni presentations focused on business achievements rather than the nuanced challenges of commercialisation within academia. Overall, they wanted to engage with alumni at key moments or when facing critical challenges to gain peer support. They sought insights on how others had overcome similar obstacles to help them achieve their final product.

CyberASAP enabled the team to apply a more commercial approach to their project, ensuring it met market needs and was sustainable. The programme also provided clarity on key priorities, such as intellectual property and legal frameworks, and will help build a solid foundation for future business growth.

'The programme has allowed us to have clarity on what is important, like being really clear with intellectual property and legal work.'

The programme enabled CyGamBIT to establish itself as a legal entity (Cyber Innovations), something that would not have been possible through the university alone. This legal status has facilitated participation in international markets and funding bids.

'*[CyGamBIT] now exists as a legal entity. We can now participate in EU bids in a way the university couldn't, which has opened opportunities for one of our directors, a professor of cybersecurity. This has allowed us to access the international market and be involved in multi-million-pound bids that the university couldn't participate in.*'

Without CyberASAP, the project lead believes CyGamBIT would not have survived due to lack of funding and commercial expertise.

'The project would not exist without CyberASAP.'

It was also suggested that beyond direct benefits to CyGamBIT, the programme also had a wider impact on Bournemouth University's Technology Transfer Office, enhancing its commercialisation process. This allowed the university's Technology Transfer Officer themselves, to broaden their network by being invited to speak at an alumni conference, highlighting the programme's influence beyond the team.

'Even our Technology Transfer Officer has benefited from this project. It has allowed Bournemouth University to elevate its commercialisation process.'

Lessons learnt from CyberASAP and wider support accessed

The project lead now takes a more strategic approach, carefully selecting team members and ensuring clarity in intellectual property and legal matters. With a deeper understanding of key business components, they integrate these into business planning and effectively align their team.

Recognising the need for cultural change within institutions was also a significant lesson. It highlighted the importance of bringing universities on board and addressing the broader context of commercialisation within academia, as many people in academia do not see research projects as products, including themselves before they became participants.

Case Study 3 – PLS-IIoT: Leveraging Physical Layer Security for Securing Industrial Internet of Things Systems

About PLS-IIoT

PLS-IIoT is a lightweight encryption method combining key generation[186] and anomaly detection[187] to protect internet-connected devices from hackers and data breaches. The team behind PLS-IIoT were involved in phases 1a and 1b of CyberASAP Year 8 having discovered the programme through an industry contact. In addition, as part of the challenge-led cohort focusing on IIoT, they received targeted support from Plexal on specific challenges facing the IIoT sector.

Context and challenges faced

The team had been researching their idea 6-7 years before involvement in CyberASAP, conducting experimental evaluations and now extending it to other wireless technologies. Their main goal was to explore commercialisation opportunities for their niche area of research in cybersecurity. They expected to learn from other academics who were also trying to commercialise their research. To date, a key challenge had been translating academic research into a proposition that would be understood by investors and industry.

'*We had no idea of [the specifics of] commercialisation and some of the steps that are needed… when it comes to the actual commercialisation, it is entirely a different world*.'

The team also hoped that – through being involved in a cyber security-specific programme – they would be able to learn from like-minded academics facing similar challenges and exploring opportunities related to commercialisation.

'We were expecting to have academics like us trying to explore the commercialisation option and learn from it.'

Support received from CyberASAP

PLS-IIoT participated in several workshops and bootcamps. The team felt the in-person workshops were beneficial, providing scope to discuss ideas and learn from speakers on concepts such as value propositions, understanding their unique selling points, and improving competitor analysis.

However, while the support provided was beneficial, it was suggested the workload required to participate in the programme alongside their day-to-day activities was overwhelming, especially alongside their full-time academic jobs. It was anticipated workshops and bootcamps would be an opportunity to meet experts and learn more about key concepts. While it was felt they were able to do this, the required preparatory and follow-up work (preparing presentation and report) was not expected.

'For a person who is already having a full-time job, teaching, marking and giving feedback… for these four months [we] pretty much worked every day alongside our full-time job.'

How CyberASAP could be improved

The PLS-IIoT team felt more could be done to maximise the academic element of CyberASAP as an academic accelerator programme. The team noted that panel members were business people who were experts in commercialisation however were not able to bridge the gap between academia and industry effectively. This created a significant challenge for the team in translating research into commercial

[186] This refers to the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted.
[187] Anomaly detection is a technique used in data analysis and machine learning to identify data points, events, or observations that deviate from the normal behaviour of a dataset.

terms. Moving forward, the team felt a stronger academic element within programme, helping to bridge the gap between academia and industry, would allow for a more streamlined approach to commercialisation.

'I think it can be improved if they add [a] more academic element to the programme… Having the academics and the commercial people in the programme [will allow them to] bridge our language.'

The team also noted that support was sometimes not tailored to their specific project, making it difficult to apply the advice. This lack of tailoring also applied to stages of development. Some participants had a fully functional project whilst they had not reached proof of concept stage and yet were participating in the same workshops. In future, the team felt separating workshops and bootcamps dependent on the participants' stage of development would help to mitigate this issue and increase the level of tailoring to individual needs. It was also suggested the second stage of the programme could be extended to allow more time for market validation and customer engagement.

In some [workshops], we don't have a proof of concept and then the others do have a working and fully functional product available, ready to go to the market. So, the sort of support they would be after would be of course 100% different than what we are looking for.

Impact and benefits of support received

CyberASAP provided them with valuable insights into the commercialisation world, which was entirely different from their academic research. They learned about market validation, value propositions, investment gathering, and how to pitch their solutions in a way that is understandable to non-technical people. The team did not feel they would have pursued commercialisation without the programme and were unsure if the likelihood of success in commercialising would have been as high, as they would not have developed the same understanding of key commercial concepts. One of the team members highlighted that academic teams they have been in contact with since participating have been impressed by their commercial understanding, demonstrating CyberASAP's positive influence.

'The success rate wouldn't be high without CyberASAP… because it prepared us for this world of commercialisation.'

However, the team are still experiencing challenges in commercialising their concept, with issues faced around pricing and confidentiality laws limiting their ability to conduct competitor analysis.

Lessons learnt from CyberASAP and wider support accessed

Although the team did not progress beyond Phase 1b of the programme, their experience in CyberASAP increased their confidence in applying to similar programmes moving forward. The experience they have gained through CyberASAP will allow them to approach future opportunities with a clearer understanding of their objectives of involvement (as well expectations for support being offered). Additionally, they felt their experience will increase the strength of future applications to similar programmes as this was their first time participating. Though the benefits of potential commercialisation in the future have not yet been realised, the team hoped that – because of being able to commercialise through support such as CyberASAP in the future – they will be able to reduce cyber attacks and increase security, reliability, and operational agility by rolling their concept out to the wider public.

Case Study 4 – ROGDRON: Rogue behaviour detection in the drone swarms using digital twins

About ROGDRON

The D-Ron (later renamed ROGDRON) platform focuses on provision of commercial and consumer drone security, where the team behind the platform highlighted a gap in the market. ROGDRON uses AI and digital twins[188] to secure drone swarms and maintain logs for drone forensics. The platform provides insurance for drone swarms by proving whether issues were caused by external actors and prevents potential hijacking. The team – which formed at Queen's University Belfast – participated in all phases of Year 6 of the programme.

Context and challenges faced

The team's main purpose for applying to the programme was to seek support in the transition from academic research to commercial entity. The team's technical background meant they were experiencing significant knowledge gaps when considering how best to pitch concepts and communicate effectively in the marketplace.

'One thing which I have seen for people who are coming from, let's say technical background like myself, is that we don't understand how [the] market talks and we don't understand how to pitch our ideas.'

Support received from CyberASAP

The team participated in several workshops and bootcamps as part of the programme. They felt the structure was well-planned and ensured manageable gaps between activities to not overwhelm or overwork the team. This also allowed the team to fit programme activities around their day-to-day roles whilst meeting all expectations set by the programme staff. The team were particularly positive about the level of clarity in how the programme was communicated, allowing them to remain aware of what was required of them.

'*We knew how many hours we need to spend on the training programme… We were aware from day one and that is the thing, you know, it really helped plan my whole semester when I was going through this programme because along with my teaching job, it was easy for me to understand when I will be away.*'

The team also benefitted from the industry expert speakers brought in as part of the programme. The team met several stakeholders from industry leading organisations such as BT, as well as members of previous CyberASAP cohorts, who's understanding of technology and provision of constructive feedback was invaluable in the team's development.

'*The number of expert speakers and trainers who were brought onto the programme and the people who I met, particularly from the likes of BT at that time and also some of their past cohorts, you could easily sense that they understand what you're talking about… they understood what we are trying to solve and what we are trying to achieve.*'

The team were particularly positive when discussing key skills learned through the programme. For example, they have been able to greatly improve their pitching ability by reducing presentation lengths and focusing on the key areas of need, which was one of their main goals for participation.

[188] A digital twin is a digital model of an intended or actual real-world physical product, system, or process that serves as a digital counterpart

'The most valuable take away has been the 5-minute pitch that I have adopted in my regular day life as well, not spending too much time on unnecessary presentations, creating unnecessary material which people just don't want to see.'

How CyberASAP could be improved

Though previous cohort members did engage in the programme, the team felt that more could be done to encourage greater alumni engagement within CyberASAP. This would allow participants / former participants to engage with those at different stages of their commercialisation journeys and better understand potential pitfalls. The team also campaigned for increased engagement of angel investors and those focused on pre-seed investment through the programme.

'They need to work more on their alumni network. That's something [that] can really help us because we also need to understand the pitfalls people have when they are moving along in this journey.'

The programme could also benefit from improved flexibility in budgeting for the projects. The team – based in Belfast – faced unforeseen circumstances such as storms which impacted their travel budget to and from London. Finally, the team suggested potential for participants who previously completed all phases to re-apply as this first experience on the programme provides valuable learning experiences which could then be applied to commercialisation at the second attempt.

When considering the influence of external factors, the team highlighted the strong role universities play in the commercialisation process – often requiring significant equity in spinouts. Moving forward, the team felt CyberASAP could play a stronger role in supporting academics by lobbying with universities to reduce equity.

'*[CyberASAP] can help lower the equity and the role and cut [the] university wants to take from these commercial activities. I think that that is something I still believe is there is scope to do a lot in that space.*'

Impact and benefits of support received

The team experienced several benefits from involvement in the programme, largely centred on developing their commercial awareness and skillsets. They have been able to meet their expectations of developing a strong value proposition and market validation which in turn allowed them to develop a prototype. Additionally, they have been able to pursue further funding and commercialisation opportunities, including via Innovate UK, to advance their prototypes to higher TRL levels. This was a significant positive outcome from Phase 2 of the programme. As well as Innovate UK, they received £100k funding as part of the Defence and Security Accelerator Programme delivered by the Ministry of Defence and have received internal investment from their university to hire another team member to support growth.

The team have applied lessons learned through CyberASAP to these subsequent commercialisation opportunities. These learnings are focused on value proposition, innovation canvas[189], and business model canvasses, as well as an awareness of the need to communicate with the right people, to these new opportunities.

'*It also put us on a journey of exploring other funding as well because certain there are certain innovate UK calls where you can use your current prototypes at a lower TRL levels to expand and go towards higher TRL. I think that was also one of the positives which came out of phase two for us.*'

[189] Home – Innovation Canvas

Additionally, the team noted increased attention being paid to their product and increased recognition for their lab regionally. Due to this increased success and interest in their work, the engineering department at Queen's University Belfast has increased engagement with the team regarding IP and equity. The team hopes this will translate into successfully licensing the technology with the university's support in the near future, and did not rule out potential for in-house investment into the platform from the university itself.

'*I'm hopeful that if I am able to, let's say licence this technology now with the help of Queens, we might see an impact case study going towards REF as well for 2029 which I think could be good… the second [option] is to look for in-house investment from Queens because they do have a commercial hub where they invest.*'

Lessons learnt from CyberASAP and wider support accessed

The future focus of the team will be to pursue investment from angel investors. Though the team have not yet received external investment, Queen's University Belfast has helped them to connect with two angel investors. However, discussions did not progress beyond preliminary phases due to the university's equity model. As such, the team have decided to halt discussions with potential investors until they have resolved any internal issues with the university. Moving forward, they are keen to explore external investment opportunities to spinout from the university and demonstrate their strong commitment to highlighting their expertise.

When considering the most significant lessons learnt from the process, the team reflected on their mindset shift from focusing on production of research without considering impact, to now considering impact at the forefront of decision making. They are now far more likely to discard ideas that may not provide societal benefit. Their focus now – and moving forward – is on building solutions with significant growth potential.

Appendix E – Activities and Outputs

The table below outlines specific activities and outputs delivered across each of the years of delivery in addition to those outlined in section 5.

Table 45: Specific activities and outputs

Year	Activities	Outputs
1	• Business plan development.	• Demonstrator showcase events for each project in Phase 2 (seven from original Year 1 cohort, and one that joined from ICURe) • Five companies formed, two acquisitions (Graphics Fuzz, Awen), and one licence (Cambridge Authentication).
2	• Pre-announcement registration of interest phase to promote programme.	• Market validation phase participation by 17 projects • One project shortlisted for funding from the Mayor of London's Civic Innovation Challenge. • Seven companies formed and two licensed (AirID and CityDefend).
3	• Pre-announcement registration of interest phase to promote programme. • X (formerly Twitter) activity and publication of articles. • Alumni conference.	• Market validation phase participation by 20 projects. • Years 1 to 3 total: three patents registered and three companies who have provided their project outputs in open-source format. • Seven companies formed and one acquisition. • One project received £200,000 in spinout support from Scottish Enterprise, and another secured £50,000 in funding from Innovate UK to develop a mobile app. • One partial participant of the programme raised £2 million in equity investment (university and angel).
4	• Pre-announcement registration of interest phase to promote programme. • X (formerly Twitter) activity and publication of articles. • Alumni conference. • 1:1 Persona Development Calls.	• 20 market validation projects. • Seven companies formed, one of which employs eight employees and in 2024 was conducting a major trial with UK Power Networks.

Year	Activities	Outputs
5	• Pre-announcement registration of interest phase to promote programme. • X (formerly Twitter) activity and publication of articles. • Alumni conference.	• Three companies formed and one company that has provided their licensed/tech available in open-source format (MLighter).
6	• Pre-announcement registration of interest phase to promote programme. • X (formerly Twitter) activity and publication of articles. • Alumni conference. • 1:1 Persona Development Calls. • TTO webinar.	• Market validation phase participation by 22 projects. • Three companies formed. • One project raised £3 million in private investment and employs ten staff (Mindgard).
7	• Pre-announcement registration of interest phase to promote programme. • X (formerly Twitter) activity and publication of articles. • Alumni conference. • 1:1 Persona Development Calls. • TTO webinar.	• Market validation phase participation by 19 projects.
8	• Pre-announcement registration of interest phase to promote programme. • X (formerly Twitter) activity and publication of articles. • Alumni conference. • 1:1 Persona Development Calls. • TTO webinar. • Introduction of a challenge-led cohort (focused on addressing market failures in cybersecurity in areas including AI model security, software supply chain security, and Industrial Internet of Things (IIOT) or Operational Technology (OT) security).	• Market validation phase participation by 18 projects.

Appendix F – 4E Framework with Tailored Performance Standards

A.1.1. Economy

Definition: CyberASAP uses resources cost-effectively (minimising overheads, administration, and delivery expenses) while maintaining sufficient quality of support for participants.

Table 46: Performance Standards for Economy

Sub-criteria	Poor	Adequate	Good	Excellent
Financial management	Budget control is weak or absent; frequent overspends or unverified costs; little sign-off or monitoring of grant disbursements.	Some budgeting exists but overspends/underspends occur without clear reasoning; checks on spend are basic.	Clear budgeting with cost controls in place, systematic sign-off on major expenses; underspends mostly explained; limited overspend.	Robust, proactive cost forecasting; each activity is tied to budget allocations; any underspend is reallocated effectively; zero financial waste.
Procurement & governance	Processes are ad hoc; duplication or inflated costs occur; volunteer contributions untracked; governance rarely addresses cost.	Some formal processes but inconsistent; some checks (e.g., TTO involvement) exist but do not systematically prevent inefficiencies.	Well-defined procurement guidelines, consistent approvals, risk assessments; partial recognition of volunteer mentors saving overhead.	Strong, multi-layered governance (TTO, external experts, DSIT) ensuring minimal duplication or cost inflation; thorough documentation of volunteer contributions.
Adaptability in design	Programme design does not respond to changing needs; continuing cost overruns or no pivot to remote/hybrid when beneficial.	Some reactive changes, but no systematic approach to cost-effective adaptations.	Active adjustment (online sessions, streamlined phases) reducing overhead while preserving participant satisfaction.	Highly proactive approach, using real-time feedback to pivot design or delivery, systematically demonstrating cost savings with no quality compromise.

A.1.2. Efficiency

Definition: CyberASAP maximises productivity by delivering intended outputs (e.g., PoCs, spinout teams) with minimal time, funds, and staff, while preserving quality.

Table 47: Performance Standards for Efficiency

Sub-criteria	Poor	Adequate	Good	Excellent
Coverage & reach	Mostly the same few universities or demographics; limited or no outreach to others.	Some variety of institutions/participants but coverage remains patchy (many unis unaware or not engaged).	Clear expansion in participating institutions (including post-92) and geographies; partial success in remote/hybrid opening access.	Broad engagement across UK, including remote/underrepresented areas; robust marketing strategy ensures high participation from a wide range of institutions.
Quality of outputs	Outputs (pitches, PoCs) are generally weak or incomplete; many do not survive investor/industry scrutiny.	Some workable PoCs, but many remain conceptual; limited external validation.	Most final demos receive positive external feedback; gating ensures only strong concepts progress, producing credible PoCs for potential investors.	PoCs frequently move to pilot or commercial deals; wide industry validation for the solutions' viability; external partners praise the technical and commercial depth.
Process & time management	Activities are unstructured or unscheduled, causing wasted resources and high dropout; participants complain about chaotic scheduling.	Some structure in phases and gating; occasional bottlenecks or confusion on scheduling, but the process generally functions.	Phased gating effectively channels resources to promising ideas with minimal wasted effort; participants rate scheduling as well-organized overall.	Highly praised scheduling with minimal rework; TTO/mentor alignment is seamless; near-zero time wasted on unproductive tasks, ensuring quick throughput.

A.1.3. Effectiveness

Definition: CyberASAP meets its core objective of commercialising academic cyber research—leading to new spinouts, viable commercial solutions, and increased investment.

Table 48: Performance Standards for Effectiveness

Sub-criteria	Poor	Adequate	Good	Excellent
High spin-out/startup formation	Very few spin-outs or licensing deals; minimal difference in commercial outcomes vs. not participating.	Some spin-outs form, but the overall success rate is modest; TTO feedback suggests partial influence from CyberASAP.	Multiple spin-outs or licensing deals each year; TTOs confirm that CyberASAP accelerates spin-out formation significantly.	A substantial portion of participants achieve spin-out or product licensing within 12–24 months; TTOs say it is a *'game changer'* for commercial outcomes.
Enhanced investment & market entry	Few or no external investment deals; industry/investors do not see programme graduates as market ready.	Some teams secure modest seed funding, but large deals or scale-ups are rare.	Many participants attract significant private investment or grants, often exceeding the programme's cost; industry generally views outputs positively.	Tens of millions in follow-on investment, high investor confidence, frequent scale-up or advanced rounds soon after graduation, widely recognised pipeline of top-tier spinouts.
Improved commercial awareness & skills	Little to no evidence of academics developing investor-savvy mindsets; TTOs note limited change from the programme.	Some participants learn basic IP/pitching but remain heavily dependent on TTO or external experts for commercial details.	Participants report confidence in pitching, IP negotiation, marketing, etc.; TTOs confirm improved autonomy in dealing with investors/partners.	Major cultural shift: academics demonstrate strong entrepreneurial acumen, produce investor-grade material independently; mentors confirm a consistent high calibre of commercial readiness.

A.1.4. Equity

Definition: CyberASAP ensures equitable opportunities and outcomes across varied universities, demographics, and regions—ensuring no key group is left behind.

Table 49: Performance Standards for Equity

Sub-criteria	Poor	Adequate	Good	Excellent
Inclusive participation	Nearly all participants from the same small group of institutions or demographics; minimal outreach to underrepresented groups.	Some variety in participants, though representation of female/minority or smaller universities remains quite low.	Notable improvement in female or minority participation; consistent outreach to post-92 or remote unis, with partial success in engagement.	Strong or near-parity representation across demographics and wide geographic spread; multiple smaller/regional institutions demonstrate high participation.
Fair distribution of benefits	Spin-outs or big wins highly concentrated in top-tier institutions, smaller or remote unis rarely see success.	Some deals or spinouts from less research-intensive unis, but the majority of success remains with Russell Group.	Clear examples of spinouts or licensing from post-92/unexpected regions; TTO changes level the playing field, though top-tier unis still dominate overall.	Spin-out success is visibly spread across the country/institutions; TTO staff confirm that smaller universities see real commercial outcomes comparable to top-tier.
Accessibility of support	In-person events predominantly in 1–2 major cities; remote or less well-resourced participants struggle to attend or fully engage.	Some partial shift to online or recorded materials, but multiple academics still cite travel burdens as a barrier.	Hybrid sessions widely adopted, lowering barriers for remote participants; in-person events remain but are supplemented by robust virtual resources.	Comprehensive accessibility measures (funding for travel or local hubs, widely available recordings/virtual events) ensure minimal disadvantage for remote or under-resourced teams.

Appendix G – Bayesian Updating

Bayesian Updating (BU) is a theory-based approach often used with CA to test contribution claims and attribute outcomes and impacts to a particular programme / policy initiative. The approach is highly flexible and can be applied to quantitative data (e.g., compliance data) and qualitative narratives, (e.g., stakeholder consultations).[190,191]

The method uses a 'prior probability' that the claim is true, and thereafter updates the assumed prior probability by assessing emerging evidence on whether an observation of success is either:

- True positive (sensitivity) - 'The probability that the evidence confirms a contribution claim is true, when it is in fact true'; or a
- False positive (Type 1 error) - 'The probability that the evidence confirms a contribution claim, when it is in fact not true'.

In the absence of strong prior evidence for the likelihood of each claim, a neutral prior probability of 50% is used, in accordance with standard practice. Bayesian updating helps in quantifying the level of confidence in a claim by incorporating new data and adjusting the probabilities accordingly.

Our evaluation focuses on the following four contribution claims:

1. **Claim A:** CyberASAP contributes to the skills and knowledge needed to turn an idea into a viable product.
2. **Claim B:** CyberASAP contributes to the skills, confidence, and knowledge needed to spin out a company.
3. **Claim C:** Participating in CyberASAP contributes to researchers attracting new investment from private and/or public sources.
4. **Claim D:** Participating in CyberASAP contributes to high survival rates of companies spun out of university research.

We have assessed the qualitative information arising from surveys, interviews, and case studies in Section 5.4. We then have converted the assessments of evidence for each of claim A to D into probability estimates, taking conservative values from ranges set out in guidance for impact evaluation.192. The higher the strength of evidence, the more confident we are that CyberASAP is having an impact. Conversely, the higher the strength of CyberASAP's contribution to the result, the lower our estimate that the results observed among participants are "false positives" attributable to other causes.

[190] EPPN-No-02-Testing-Contribution-Claims-with-Bayesian-Updating-.pdf
[191] Diagnostic evaluation and Bayesian Updating: Practical solutions to common problems
[192] Befani, B., & Stedman-Bryce, G. (2016). Process Tracing and Bayesian Updating for impact evaluation. *Evaluation*, *23*(1), 42-60. https://doi.org/10.1177/1356389016654584 (Original work published 2017)

Table 50: Quantitative assessment of strength of evidence

Assessment of strength of evidence	Probability of CyberASAP impact	Probability of "false positive"
Moderate	60%	40%
Moderate to strong	67.5%	32.5%
Strong	75%	25%

We have also sought external quantitative information to compare with surveys and management information to add to the evidence base for each claim. Using publicly available secondary data, we have developed the following baseline estimates:

1. **Claim A: Viable product.** Historical surveys and HE-BCI data suggest that, without structured support, only a small fraction of academic research projects progress to a market-validated or viable product stage. Indicative baseline: ~5%[193]
2. **Claim B: Spin-out formation.** Data from HE BCI indicate that the proportion of academics who spin out a company is very low – often well under 1–2% annually – reflecting the challenges of transitioning research into commercial ventures independently. Indicative baseline: ~1-2%[194]
3. **Claim C: Attracting investment.** Analyses from Beauhurst and sector studies show that, in early-stage academic spinouts, securing external investment is challenging, with only around 10–15% attracting significant private or public funding in the early years. Indicative baseline: ~10-15%.[195]
4. **Claim D: Company survival.** UK small-business and spinout data suggest that survival rates for academic spinouts can be relatively high (around 60–70% over three years) due to strong intellectual property and university backing, though long-term growth remains challenging. The indicative baseline is ~60-70% (3-year survival). This is higher than for start-ups in general; research indicates that approximately 57% of start-ups have dissolved within 2 years across the time period of CyberASAP[196].

This data gives strong contextual evidence for the effectiveness of CyberASAP, but it varies for each claim.

For Claims A and B, the success rates for Cyber ASAP participants generating viable products and forming spin-outs are much higher than for the general academic population. However, the general academic population success rate cannot be directly compared to the success rate of CyberASAP in achieving the outcomes referred to in the claims. This is because of a selection effect – only those academics with potentially commercialisable IP or an interest in forming a start-up will apply for CyberASAP. Many academics do not generate commercialisable IP over their careers and might prefer to pursue their research career rather than investigate the spin-out career path.

However, for Claims C and D, spin-outs arising from CyberASAP can be compared to the relevant populations (spin-outs and innovative companies seeking investment and growth).

30% of CyberASAP spin-outs in our survey reported that they had secured investment. In the management information, 23 out of 29 start-ups in cohorts 1-5 had secured at least some investment (79%), although 6 had secured markedly less than others, at under £50,000 (the remainder, 17/29, represents 59% of the sample). This gives 3 varying estimates of the probability that CyberASAP spin-outs secure investment; we

[193] HESA HE-BCI Survey (hesa.ac.uk), Centre for Business Research historical surveys (e.g. Cambridge studies, link available upon request)
[194] HE-BCI Survey (hesa.ac.uk)
[195] Beauhurst (beauhurst.com),
[196] PwC analysis finds failure rates amongst startups at lowest level in a decade, despite record company formations

have elected to use the central estimate of 59% for this analysis, on the grounds that the very low investment amounts in management information could be personal resources or family members etc rather than significant external investment. With regard to Claim D: out of 29 spin-outs in cohorts 1-5 for which we have been given management information, 3 have been dissolved (10.3%) and 2 are reported as dormant (6.9%). The survival rate is therefore between 89.7% and 82.8% depending on whether the dormant companies are treated as having not survived. We have adopted the midpoint of these two estimates for this analysis.

Claim A: CyberASAP contributes to the skills and knowledge needed to turn an idea into a viable product.

	Strength of contribution	Strength of evidence	P (E|H)	P(E|¬H)	Bayes factor
Enables	Strong	Strong	0.75	0.25	3
Enhances	Moderate to Strong	Strong	0.75	0.325	2.31
Fosters	Strong	Moderate	0.6	0.25	2.4

Posterior probability: 94%

Claim B: CyberASAP contributes to the skills, confidence, and knowledge needed to spin-out a company.

	Strength of contribution	Strength of evidence	P (E|H)	P(E|¬H)	Bayes factor
Builds confidence	Strong	Moderate to Strong	0.625	0.25	2.5
Connecting	Strong	Strong	0.75	0.25	3
Licensing instead	Moderate	Moderate	0.6	0.4	1.5

Posterior probability: 92%

Claim C: Participating in CyberASAP contributes to researchers attracting new investment from private and/or public sources.

	Strength of contribution	Strength of evidence	P (E|H)	P(E|¬H)	Bayes factor
Ability	Strong	Strong	0.75	0.25	3
Market alignment	Moderate to Strong	Moderate	0.6	0.33	1.84
Credibility	Strong	Moderate	0.6	0.25	2.4
Investment rate	10-15%	{30%,59%,79%}	0.59	0.15	3.9

Posterior probability: 98%

Claim D: Participating in CyberASAP contributes to high survival rates of companies spun out of university research.

	Strength of contribution	Strength of evidence	P (E|H)	P(E|¬H)	Bayes factor
Long-term survival	Moderate to Strong	Moderate	0.6	0.325	1.85
Network effects	Moderate	Moderate	0.6	0.4	1.5
Survival rate	60-70%	83-90%	0.86	0.65	1.32

Posterior probability: 79%

Appendix H – Real Value of Costs

We have converted all nominal (cash) spending in each financial year to 2024/25 prices using a GDP deflator index. In this approach, 2024/25 is set to an index of 100, and each earlier year's index is below 100, reflecting lower price levels historically. The formula is:

Adjusted spend (2024/25 prices) = Nominal spend in year t × (100/ Deflator index in year t)

Table 51: Annual nominal spend, deflator index, and resulting adjusted spend in 2024/25 prices.

Year	Budget (£)	Nominal spend (£)	Deflator Index (2024/25=100)	Adjusted spend (£)
2018/19	2,144,523	1,515,993	79.26	1,912,569
2019/20	2,655,040	1,577,907	81.14	1,944,604
2020/21	1,967,600	1,561,735	85.50	1,826,662
2021/22	1,383,032	1,061,506	85.00	1,248,873
2022/23	1,495,500	1,326,295	90.99	1,457,578
2023/24	2,117,388	1,522,033	96.34	1,579,884
2024/25	2,286,990	1,227,769	100.00	1,227,769
Total	14,050,073	9,793,238	–	11,197,940

Source: Historic GDP deflator data from ONS March 2025. 2024/25 prices forecast from OBR GDP deflator forecasts as of March 2025. Budget and spend from DSIT internal records and CyberASAP budget documents. Minor rounding differences may occur.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM UK Consulting LLP
The Ewart
4th Floor
3 Bedford Square
Belfast
BT2 7EP
United Kingdom
T +44 (0)28 90234343
rsmuk.com