DPS Schedule 6 (Order Form Template and Order Schedules)

Order Form

ORDER REFERENCE:	Con_5680 – Team UK and UK Cyber Competition Programme
THE BUYER:	The Department for Science, Innovation & Technology
BUYER ADDRESS	10 Victoria Street, London, SW1H 0NB
THE SUPPLIER:	SANS EMEA
SUPPLIER ADDRESS:	Unit 5, Enterprise Park, Atlantic Cl, Swansea, SA7 9FJ
REGISTRATION NUMBER:	**12676167**

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 15th March 2024 It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

DPS FILTER CATEGORY(IES):
Not applicable

ORDER INCORPORATED TERMS
The following documents are incorporated into this Order Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Order Special Terms and Order Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM3764iii
3. The following Schedules in equal order of precedence:

   - Joint Schedules for RM3764iii
   - Joint Schedule 2 (Variation Form)
   - Joint Schedule 3 (Insurance Requirements)
   - Joint Schedule 4 (Commercially Sensitive Information)

- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 7 (Financial Difficulties)
- Joint Schedule 8 (Guarantee)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

- Order Schedules for RM3764iii
  - Order Schedule 4 (Order Tender)
  - Order Schedule 5 (Pricing Details)
  - Order Schedule 7 (Key Supplier Staff)
  - Order Schedule 20 (Order Specification)

4. CCS Core Terms (DPS version)
5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
6. Annexes A & B to Order Schedule 6
7. Order Schedule 4 (Order Tender) as long as any parts of the Order Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Order Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

ORDER SPECIAL TERMS
The following Special Terms are incorporated into this Order Contract:
None

ORDER START DATE:	**18th March 2024**
ORDER EXPIRY DATE:	**31st March 2025**
ORDER INITIAL PERIOD:	**1 Year**
ORDER OPTIONAL EXTENSION	None

DELIVERABLES
See details in Order Schedule 20 (Order Specification)

MAXIMUM LIABILITY
The limitation of liability for this Order Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is [redacted]

ORDER CHARGES
See details in Order Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES
Recoverable as stated in the DPS Contract

PAYMENT METHOD
BACS Transfer

BUYER'S INVOICE ADDRESS:
DEPARTMENT FOR SCIENCE, INNOVATION & TECHNOLOGY (DSIT)
C/O UK SBS
QUEENSWAY HOUSE
WEST PRECINT
BILLINGHAM

[redacted]

BUYER'S ENVIRONMENTAL POLICY
Attached as Appendix A

BUYER'S SECURITY POLICY
Attached as Appendix B

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]

Sans Institute,
Ty Davies Tawe Business Village,
Swansea Enterprise Park,
Swansea,
United Kingdom
SA7 9LA

SUPPLIER'S CONTRACT MANAGER

[redacted]

Sans Institute,
Ty Davies Tawe Business Village,
Swansea Enterprise Park,
Swansea,
United Kingdom
SA7 9LA

PROGRESS REPORT FREQUENCY

As outlined in Order Schedule 20 (Order Specification)

PROGRESS MEETING FREQUENCY

As outlined in Order Schedule 20 (Order Specification)

KEY STAFF

[redacted]

Sans Institute,
Ty Davies Tawe Business Village,
Swansea Enterprise Park,
Swansea,
United Kingdom
SA7 9LA

KEY SUBCONTRACTOR(S)

[redacted]

COMMERCIALLY SENSITIVE INFORMATION

All background IP remains confidential and commercially sensitive to SANS.

SERVICE CREDITS

Not applicable.

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the Deliverables and performing its obligations under the Order Contract, that it will comply with the social value commitments in Order Schedule 4 (Order Tender)]

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	[redacted]	Signature:	[redacted]
Name:	Marc Anson	Name:	Cian Galvin
Role:	General Counsel	Role:	Acting Deputy Director, Cyber Inn
Date:	28/3/2024	Date:	28/3/2024

Order Schedule 4 (Order Tender)

DEPARTMENT FOR SCIENCE, INNOVATION, AND TECHNOLOGY

Team UK and UK Cyber Competition

Ref. No: ITT:51120

Technical Submission:

SANS Institute
February 2024

Section One: Relevant Experience

SANS are the world leaders in cutting edge cybersecurity training, certification, and Cyber Ranges. SANS' expansive catalogue of Ranges vary from foundational challenges aimed at newcomers to the industry, to highly technical, specialised testing for the most seasoned practitioners. Further information on the proposed Ranges for inclusion in this project are outlined in the response to Q3.

SANS Training UK Ltd is a wholly-owned subsidiary of SANS which operates in 128 countries. SANS is divided into six regional sites: UKINI, APAC, the US, META, Mainland Europe and Latin American, each with their own dedicated teams partnering with governments and private organisations to run a comprehensive range of training, CTF exercises, and customised programmes. The team leading this programme will be based in the UK, with access to the breadth of knowledge and skills across each of the SANS regional sites.

Planning, designing and successfully participating in major international cyber competitions

SANS Cyber Ranges are regularly featured at cybersecurity events and conferences, including the annual CyberThreat conference delivered in partnership with the National Cyber Security Centre (NCSC). Led by James Lyne, SANS' Chief Technology and Innovation Officer, the conference prioritises technical expertise, real-world case studies, and introduces new security tools.

It includes a technical CTF range by SANS and hands-on challenges provided by partner [redacted] Participants engage in online CTF-style competitions before the event, with chances to win tickets. The CyberThreat CTF offers a narrative-based, immersive experience across cloud systems, hardware, and interactive 'hackable badges'.

Youth engagement and retention: In the UK, SANS partnered with DSIT, (then DCMS) to deliver the Cyber Discovery programme, engaging over 100,000 13-18 year-olds in interactive cybersecurity training over four years. SANS designed the programme to be enjoyable and engaging, offering interactive challenges, labs, and learning materials through platforms like CyberStart and SANS Foundations.

Using a gamified approach, participants assumed the role of cyber agents within the narrative of the 'Cyber Protection Agency', learning real-world cybersecurity techniques. Thousands remained committed to vie for selection to attend in-person training events, fostering a sense of community among young cybersecurity enthusiasts.

SANS also works closely with military organisations to prepare participants for the Services Cup, a CTF competition for elite teams from various countries.

Designing and conducting knowledge, capacities, and skills-related gaps/needs assessments

SANS, in collaboration with psychometricians and cybersecurity experts, developed assessment tools to evaluate individuals' cybersecurity skills and aptitude across various domains. These assessments cover Cloud Security, Cyber Defence, Penetration Testing, Application Security, Digital Forensics, Industrial Control Systems, Management, Technical Comprehension, Problem Solving Skills, and Knowledge Application. By utilising these tools, SANS identifies suitable training plans for security practitioners and has identified individuals with potential for success in cybersecurity careers in recent UK reskilling programmes. [redacted] demonstrating the tool's effectiveness in predicting success and identifying candidates with potential.

Designing and developing training content and material

In response to the need for tailored training for UK employers, SANS' UK-based Programmes team designed a 10-week training programme, Upskill in Cyber, offering various learning modalities, expert support, and opportunities to engage with industry practitioners. The programme included support from Subject Matter Experts, Mentors, and a Pastoral Care team, as well as career preparation assistance such as Career Fairs and CV and Interview support. This comprehensive approach ensured that individuals from diverse backgrounds, learning styles, and circumstances could succeed. Additionally, based on feedback and insights, bespoke extra-curricular support was provided to ensure a solid understanding of technical concepts. Identified areas for support were addressed through action plans agreed upon by SANS practitioners and industry representatives, with virtual sessions and mentor support implemented accordingly. For instance, participants struggling with programming received additional sessions with a dedicated practitioner for personalised tutoring.

Identifying and securing the continued active engagement of key project stakeholders

Since 2015, SANS has executed over 200 programmes and a critical aspect of each is the partnerships with industry. One of the most notable of these in the UK is the Upskill in Cyber programme on behalf of UK Government, engaging with over 150 organisations to input into soft skills development of participants and to raise awareness of employment opportunities and pathways into cyber. In excess of 70 of these employers have been supporting SANS programmes since 2015.

This has been achieved through comprehensive marketing campaigns and fostering relationships through 1:1 engagement with industry to understand their needs, ensuring partnerships benefit the organisation and participants, therefore securing continued support and engagement.

Present and future international cyber competition landscape

SANS possesses a comprehensive grasp of the international cyber competition landscape, achieved through market research, technical expertise, and competitor analysis. They meticulously monitor existing competitions, their formats, and the emphasised technical skills, ensuring their programmes remain pertinent and competitive. By scrutinising competitors' strengths and weaknesses, SANS identifies areas for differentiation and enhancement, while also staying abreast of emerging trends and future prospects in cybersecurity. Feedback mechanisms and collaborations with industry partners further enrich their understanding, enabling SANS to adapt their programmes to evolving needs and expectations, ultimately providing a cutting-edge platform for cybersecurity education and training tailored to the next generation of professionals.

Project planning, design, and implementation & Project monitoring, evaluation, and learning

SANS' UK Programmes Team oversees project planning, design, implementation, monitoring, evaluation, and learning. With experience since 2017, they've managed various government programmes like the Cyber Retraining Academy and Cyber Discovery. Using a robust project management structure, they ensure effective delivery, risk management, and stakeholder engagement. Continuous review and refinement based on self-evaluation and stakeholder feedback enhance project outcomes, as seen in initiatives like Upskill in Cyber, where adjustments to the onboarding process improved programme effectiveness and participant outcomes. SANS also engage with external evaluators where required.

Section Two: Organisational competencies and capacities

Technical and thematic knowledge, experience, skills, and expertise

SANS’ global prominence places us in a unique position to be able to deliver on this project. SANS training is authored and taught by world-class cybersecurity experts who are passionate about their chosen subject areas. SANS Instructors must be actively working in their field to be able to teach, ensuring that real-world experiences are brought into all aspects of training.

Training and skills development management

SANS have proven experience in leveraging this expertise in identifying, understanding, and responding to emerging threats. SANS operate the Internet Storm Center, known as the internet’s ‘early warning system’ for emerging threats. The service shares over 20 million intrusion detection log entries, per day, in real time, and is used by security practitioners worldwide to understand new threats and tested mitigations.

In addition to core training, SANS provide, at no cost, access to thousands of security resources, tools, podcasts, newsletters, and free events. SANS develop and provide more training and CTF content than any other organisation globally, and the community have regular opportunities to access CTF challenges and to practice their skills at no cost.

The following senior individuals, all UK based, will be responsible for the delivery of this project.

[redacted]

[redacted]

[redacted]

Other key personnel or physical resources

SANS are committed to delivering this project with proactive industry and academic involvement.

[redacted]

[redacted]

An advisory board of cyber experts, including globally renowned authorities [redacted] will contribute to the project's design and scope. Their extensive experience in penetration testing, incident response, and advanced exploit development adds depth and expertise to the initiative.

Project management and governance

SANS' dedicated Programmes Team design, implement, and monitor a range of initiatives, which aim to raise awareness of security careers, improve prospects for individuals, provide theoretical and hands-on training for practitioners and strengthen the security of local employers and nations. The UK-based team provide bespoke programmes to the private sector, military organisations, and Governments with the UK, Europe, and the Middle East.

Operating as an Agile project team utilising key project management principles and approaches, the team can respond to changing needs from a range of stakeholders. Reporting and communications are agreed on a basis to suit individual stakeholders with frequency, method of reporting, and level of detail all flexible options.

Resource and risk management & Monitoring, Evaluation, and Learning

Programmes are thoroughly planned using project management software and progress against priorities, potential risks and mitigations, and opportunities for improvement are logged and reported into the relevant stakeholders. Risk scanning takes place throughout the project lifetime, with clear triggers for escalation and communication to appropriate stakeholders, including internally, when necessary.

Throughout planning and delivery, the team seek regular feedback from key partners, participants, and the client to identify strengths and areas for improvements.

Key stakeholder engagement and management & partnership management

The SANS Programme team engage with stakeholders at all levels to understand the main objectives and outcomes, allowing a tailored solution with a holistic approach consisting of marketing and communications, existing and, where appropriate, bespoke training, certifications, extra-curricular support, and engagement with industry and academia. SANS intend to recruit a dedicated Industry and Partnership Manager for this project, who will oversee this project requirement.

SANS also have access to additional in-house resources to support the successful delivery of this contract.

Contract management and compliance

Legal Counsel and Data and Compliance teams can oversee contract, data sharing and protection requirements.

Comms and marketing

The in-house Marketing and Design team will develop a marketing strategy and implement a comprehensive campaign to attract potential participants, industry, and academia, as well as a strong brand for the programme.

Event management

The Event Management Team will also be utilised to support planning and execution of in-person events. The team deliver hundreds of events globally, from private training classes, multi-class events, and global conferences and summits, including the annual CyberThreat conference.

Section Three: Understanding the Requirement

Project management and governance

The programme team is adept at working with different methodologies, tailoring the delivery of projects accordingly depending on stakeholders' knowledge and experience and can work with them to identify the most appropriate delivery method. SANS will opt for a blend of Agile and Prince2 for this project. By blending Agile and Prince2 methodologies, the team aims to leverage the strengths of each approach. Agile's iterative development and testing approach will allow flexibility and responsiveness to evolving needs, ensuring the solution is optimised throughout the project lifecycle. Meanwhile, Prince2 will provide structured frameworks for controlled environments, enabling effective governance and oversight of the project as a whole. This combination will facilitate efficient project execution while maintaining governance and control over project activities.

Regular communication and reporting with DSIT, ongoing risk management, daily reviews against key milestones, and proactive adjustments made to delivery, will all contribute to ensuring success at all phases of the programme. All timescales and key deliverables are monitored using Prince2 principles, providing the necessary governance to ensure delivery on time and within budget. Work is planned in stages to ensure control on project progress, and our extensive experience with previous programmes means we have a good understanding of managing and controlling each stage. The project manager will agree with the board, and implement, project tolerances at the outset, with robust monitoring and reporting internally, to allow for efficient delivery. Regular reviews are conducted by SANS management and the programme team, as part of our strict governance regime, with regular reporting to the board – this can be as frequently as every day in the early stages of a programme but, typically, on a weekly basis through a project highlight report.

Roles and responsibilities are clearly defined, which leads to a robust system for dealing with any issues as they occur or are raised, limiting impact on the project timeline. CTF Ranges and platforms are already in place and ready to launch, whilst the programme team is ready to be mobilised. A RACI and agreement of a Stakeholder and Engagement Approach will be agreed with regular feedback mechanisms implemented. The interdependencies have already been mapped to ensure we have an early grip on all aspects of the programme and to minimise the risks. Any contingencies triggered during the programme will be implemented at our cost.

Project reporting and comms

As outlined in the response to Q2, SANS' dedicated Programmes Team will manage stakeholder engagement, identifying partners and contributors who are responsible and accountable for decisions, and those that need to be consulted or informed, as well as agreeing suitable methods and frequencies for engagement. The team will manage project plans and will be held accountable to an internal Programme Manager, the Project Board, and DSIT. As part of project planning and management, the team will closely monitor risks from all aspects of the programme and ensure reasonable mitigations are built in where appropriate, or impact successfully minimised. The team will be responsible for ensuring the project is delivered on-time and on-budget.

Throughout previous training programmes delivered for UK Government, SANS has provided regular reporting on collected data, successfully delivering to the Service Level Agreements in place. The programme team has transparent procedures for collecting, processing, and reporting of data through clear communication channels. There are dedicated staff who undertake data collection, including from industry partners, where appropriate. This activity will be led and overseen by [redacted] Programme Manager, with the support of the programme team; she will be supported by a Senior Project Coordinator responsible for ensuring weekly reporting to DSIT on progress, on analysis of what the data is showing, and for ensuring any emerging issues are shared immediately. A flexible approach will be adopted throughout to meet DSIT's needs.

Various proven tools will be utilised to ensure communication and reporting is successful during the programme, through provision of relevant, real-time qualitative and quantitative data on participant progress. All emails received from DSIT will be responded to in a timely manner by the dedicated point of contact, as all previous programme engagement with UK Government has shown. Following the Project Initiation Meeting, regular contact will take place between the Service Provider and the Authority by video call, telephone, email, and face-to-face meetings as required.

Finance, resource, and risk assessment and management

Experienced replacements have been identified for the key personnel listed in the response to Q2, as a contingency. Several measures have been factored in to minimise or eliminate the impact of other key staff changes, namely: the Cyber Ranges team responsible for the delivery of the technical CTF rounds, and the core delivery team responsible for recruitment and selection, marketing, Industry and Academic partnerships, event planning and participant support.

On average, SANS will deliver [redacted] live and online training events reaching over [redacted] globally each year. Staff absence is a potential risk at each of these events and processes are embedded into planning to allow the SANS teams to replace staff at short notice. Uniformity across planning processes and use of tools ensures that the impact posed by staff changes is mitigated at pace and significantly reduced. Cloud-based project management tools are used to capture individual responsibilities, tasks, and deadlines; accessible anytime. This provides instant oversight of agreed timelines, and whether adjustments in allocation of resources are needed to ensure success. Files are stored in company-wide cloud storage, with access permissions granted to relevant team members. Slack is used by all SANS' employees, with private channels for individual projects, providing a dedicated space for team discussions. SANS also have significant event management and marketing resources that can be re-allocated within EMEA. Any new team members are provided with access to project management tools and files and can quickly get up to speed on the current status of a project and outstanding tasks.

The programme's financial management will be a top priority for the team, given the ambitious requirements and limited budget. SANS' proposed solution has a commercial value exceeding [redacted], and as such, will meticulously manage finances to ensure its viability and maximise its impact. The team will adopt a strategic approach, segmenting programme elements that are more likely to attract sponsors and partners' interest, such as live finals and international competitions, to support execution effectively. Additionally, SANS will maintain a profit and loss (P&L) statement, diligently tracking all internal and external costs throughout the programme's lifecycle to ensure financial viability and accountability.

SANS' experienced programme management team has the necessary expertise and tools to manage this type of programme, including the identification, mitigation, and management of risks. A risk register is established at the outset of any programme and is updated on a regular basis, noting any new risks and mitigations, or changes to existing ones. Programme risks and mitigations identified will be agreed with DSIT at the outset of the programme, with regular updates provided at agreed intervals. Any significant new risks identified will be reported upon discovery, along with our approach to mitigation. [redacted] will have overall responsibility for managing risk. Notable risks, with a brief outline of their mitigations, are included at the end of this section. During the refinement of the project scope, a comprehensive risk register and mitigation plan will be scoped but key risks are below.

Monitoring, Evaluation, and Learning Plan

Essential to the delivery of this programme is insight, feedback, and appropriate challenge from relevant partners. Throughout planning and delivery SANS will review feedback from key partners, participants, and DSIT to identify strengths and areas for improvements. This will be through quantitative and qualitative data including metrics used to measure the success of marketing and communications, diversity monitoring, stakeholder surveys, informal feedback and group discussions and responses received to feedback requested by independent evaluators. SANS will also self-evaluate internally to ensure that processes are efficient and that the project is on track to achieve its outcomes.

Project records will be made available via secure, online platforms to ensure that data is readily available and accurate at all times to relevant stakeholders and evaluators. A 'lessons learned' log will be accessible to stakeholders who can provide feedback (anonymously if they wish) with SANS review and recommended actions published and visible for all.

Progress and success will be measured by the following criteria:

- Establishing an Industry Advisory Panel with academia and industry from a variety of sectors
- Establishing a Youth Project Group with a diverse pool of young people, including gender, ethnicities, backgrounds, and neurodiversity
- The number of participants registering for the warm-up round
- The number of participants remaining engaged for the semi-final and in-person final rounds
- A variety of partners attracted to provide sponsorship and services in kind
- Outcomes of satisfaction surveys from participants and partners
- Onboarding of partners to highlight educational and career pathways
- Selection of a team with a diverse set of skills and experience and high aptitude
- Improved/sustained physical and mental health of stakeholders
- Performance in local and national cyber competitions
- Team UK's readiness for participation in international competitions
- Commitment from industry and academia to continue to support the programme after 12 months

Project information and data management/protection

SANS ensures full compliance with GDPR, the Data Protection Act 2018, and UK laws and regulations, holding Cyber Essentials Plus and ISO 27001 certifications. Oversight by our dedicated Data Protection Officer, is subject to periodic QA audits, guarantees adherence to controls and processes.

As required, SANS are willing to complete a Data Protection and Impact Assessment (DPIA) as previously implemented for similar projects like Upskill in Cyber. Stringent controls and processes secure data and communications at every stage, from collection to destruction. Sensitive data is password-protected, stored securely, and accessed only by authorised staff through approved channels.

Staff undergo comprehensive training to handle sensitive information securely, fostering trust from learners, clients, and governments across 28+ countries. With automated backups for data loss, we have various recovery methods and response times for incidents, treating data breaches as business continuity issues. We follow ICO best practices, and will promptly notify affected parties, DSIT, and ICO within one day of awareness of any breach, conducting post-incident analyses and implementing necessary rectifications.

Where relevant and possible, the programme design meets the Technology Code of Practice, detailed throughout the bid response.

A clear and detailed workplan for the full project period providing key activities and deliverables, associated timelines, key dependencies, and assumptions/comments. *A full project plan is available on request.*

Upon contract award, SANS will thoroughly scope the solution for participant and partner attraction, delivery of the large cyber competition, and team selection, development, and training. A high-level programme plan outlines the intended delivery. Key partners will be engaged from the outset to ensure the proposed solution meets overarching aims and effectively assesses and selects suitable candidates for Team UK. SANS will establish an Industry Advisory Panel comprising technical experts and external partners from industry and academia to provide counsel on key decisions, such as proposing team-based CTFs at the in-person final for evaluating team working skills. Regular meetings and an online noticeboard will keep panel members informed and facilitate feedback. A Youth Advisory Panel will be formed, including individuals aged 18-24 who participated in the Cyber Discovery programme and the Cyber Security Council’s youth group. They will offer insights on the cyber competition, programme messaging and branding, and ways to enhance opportunities for accessing cybersecurity education and careers. Following design and stakeholder feedback, implementation will commence with ongoing engagement to assess impact and early outcomes.

Key Project Deliverables

Research and Recruitment Gathering

SANS will employ a meticulous requirements gathering approach to ensure that all stakeholders’ needs are thoroughly understood and addressed. This process will begin with comprehensive stakeholder engagement, involving key representatives from various sectors, including government, industry, academia, and potential participants. Through structured interviews, surveys, workshops, and focus groups, SANS will elicit valuable insights into stakeholders' expectations, preferences, and priorities. Additionally, SANS will conduct thorough market research and analysis to identify emerging trends, technologies, and best practices that may influence the project's requirements.

Moreover, SANS will incorporate robust testing and feedback loops throughout the project lifecycle to validate requirements and inform reviews of solutions. Example programmes will be developed and tested in collaboration with stakeholders to gather real-world feedback and insights. This iterative approach will allow for continuous refinement and improvement based on stakeholder input, ensuring that the final solution meets or exceeds expectations.

Comms and marketing

Development and launch of the Creative Strategy, Campaign, and Brand

The SANS Marketing and Design team will work closely with the DSIT Comms team – and external agencies if deemed appropriate – to develop the marketing and communications approach, to include recruitment and engagement of participants and programme partners and sponsors. Research will be undertaken to understand the motivations for young people to participate in this kind of programme and to develop messaging and creative that will resonate with them, encouraging them to apply and participate. SANS would seek to utilise testing with the target audience to ensure that messages land and Calls to Action to participate will be successful. [redacted]. The Industry Advisory Panel and organisations from SANS' extensive UK customer base can also be drawn on for feedback on the partner side of the campaign.

This feedback and insight from the target audiences will ensure the overarching strategy, intended outcomes, implementation plans, and metrics to measure success will be suitable to attract a diverse pool of participants to apply, and a range of industry partners who can provide valuable input to the delivery of the programme. They will also be critical in ensuring that the programme brand is strong and attractive to potential applicants and to industry to encourage their sponsorship and buy-in.

The implementation will include a combination of paid activity and low and no-cost options. Paid activity will utilise press, social media, and mailings on both the participant and industry campaigns.

Unique to SANS are our existing partners and networks which can be leveraged in our no-cost approach. These include:

Organic Social
Project Partners
[redacted]

[redacted]

Participant Attraction

The marketing campaign will be designed to attract a diverse pool of candidates to apply, ensuring that benefits of participating are clearly communicated to incentivise engagement. One of these incentives will be to attend the SANS and NCSC CyberThreat Conference in November 2024, which will also be useful training for the top 50. SANS' partner, [redacted] will develop a series of 'teaser' challenges which will provide an insight to the types of challenges individuals can undertake if they register to participate. Some of the developers at [redacted] fall within the 18-25 year old category, meaning they can design these challenges to be engaging and relevant for the target audience. This should help to maximise the number of applicants at the entry stage, ensuring a large and rich talent pool to select from.

Partnership management & Key stakeholder identification, engagement, incentivisation, and management

Partner Attraction

Partner attraction is a key dependency for this project's overall success**.** A dedicated Industry and Partnership Manager will establish and maintain relationships with key partners on the Industry Advisory Panel and wider contacts within industry and academia. Packages of support options will be developed to provide a range of options for industry to get involved with the programme, with feedback from industry and academic partners to ensure they are suitable and will incentivise participation. Options will allow partners to buy into the programme, either financially or with services in kind. These options could include mentorship, the opportunity to deliver training sessions for Team UK, deliver sponsored sessions about an organisation and career opportunities, the ability for organisation's employees to participate in the CTFs as part of their professional development, merchandise sponsorship and the chance to sponsor the live final, the teams' travel to international competitions and the naming of Team UK.

Academic partners may also be interested in highlighting potential educational pathways to get into the cybersecurity industry. Partners will also be able to suggest support options to ensure that partnerships are beneficial for all stakeholders. This will also be critical in ensuring that the team are sufficiently funded to able to travel to competitions and can access new tools and resources as required.

Partnership Management

Throughout the project, SANS will implement a comprehensive partner management strategy to ensure effective collaboration and alignment with project objectives. This strategy will begin with clear and transparent communication to establish a mutual understanding of roles, responsibilities, and expectations. Regular meetings and progress updates will be conducted to maintain ongoing engagement and alignment with partners' goals and priorities. Additionally, designated points of contact will be assigned to facilitate efficient communication and address any issues or concerns that may arise.

Collaboration tools and platforms will be utilised to streamline communication and document sharing, fostering a collaborative and cohesive working environment. SANS will also seek feedback from partners to improve processes and continuously address any areas for enhancement. By prioritising proactive and transparent partner management, SANS aims to foster strong and productive relationships that contribute to the project's success.

Event management

Delivery of a virtual 'warm-up' round

To ensure this first stage is accessible to individuals of all skill levels and that SANS can raise awareness of cybersecurity careers amongst the wider participant group, the first round will utilise the SANS BootUp! CTF Cyber Range. This CTF was designed for entry-level practitioners and offers hints and guidance to assist progress and push players to research information outside of their current knowledge base. Players will also be signposted to suitable, free resources for CTF play in an effort to improve the skill levels of all participants. The CTF only requires access to an internet connected machine which should maximise the number of participants able to access the round. SANS will aim to attract a minimum of 1,000 participants for this first stage to account for dropouts and to ensure a large enough pool to progress to subsequent stages and finally selection. Analysis of individual performance will commence at this stage so that SANS can build a picture of individuals' baseline skills and can therefore track progress throughout the competition, as this will be an important consideration in final selection alongside skill level.

Raising Awareness of Cyber Pathways and Opportunities

Individuals attracted to participate in this programme will have a keen interest in cybersecurity or will be new to the sector. Regardless of their background and performance in the programme, SANS will endeavour to ensure that all participants gain a better understanding of the opportunities available to them. This will include signposting to suitable resources and opportunities from SANS and other reputable partners, access to support from the [redacted]. All participants will be invited to attend virtual industry events to learn more about the work that cyber practitioners do.

Delivery of a semi-final round

The semi-final round will invite the top 400 participants from the warm-up round to participate in the more advanced Core NetWars CTF Cyber Range. NetWars challenges test a wide variety of disciplines and subject matter across 5 levels that increase in difficulty but does feature an automated hint system to help participants solve questions they may find particularly difficult. Increasing the difficulty at this stage will allow SANS to begin identifying potential participants to watch out for and to start identifying strengths and weaknesses that may need to be addressed within the top 50 training.

Delivery of the in-person final round

The top 200 participants from the semi-final round will be invited to attend the in-person final which will resemble an 'e-sports' style event with an impressive audio-visual set up and ability for the audience to watch the leaderboard from a large screen. The CTF delivered at this stage will be a highly technical, narrative-based Cyber Range, such as Jupiter Rockets or TelNet. Either of these ranges will be suitable for accessing the top level of talent in the competition, requiring students to work in teams of 4-5 players to solve challenges. This will allow SANS to consider not only the participants' individual performances but assess how they interact and work as a team, a critical element that must be evaluated prior to the selection of Team UK. The 'ladder' style championship model, increasing in difficulty and reducing in participant numbers will act as a strong motivator for participants to remain engaged in the programme. This will also allow SANS to become better acquainted with the participants on a personal level and understand their motivations for participating.

Training and skills development management

Understanding the cybersecurity landscape: The landscape for national and international CTF competitions is dynamic and highly significant for several reasons, particularly in the context of national defence, foreign relations, and services export.

National CTF competitions are typically organised within a country and are often aimed at identifying and nurturing local talent in cybersecurity. They serve as a platform for students, professionals, and enthusiasts to demonstrate their skills in areas like network security, cryptography, web vulnerabilities, reverse engineering, and other domains relevant to digital security. These competitions often receive support from government bodies, educational institutions, and private sector companies, reflecting a collaborative effort to strengthen national cybersecurity capabilities.

Winners of national competitions advance to represent their country in international competitions, such as DEF CON CTF, the European Cyber Security Challenge, and the Trend Micro CTF. These events, drawing participants from multiple countries, offer a larger scale and diverse security challenges, fostering a global exchange of knowledge and skills. Success in international CTFs signals a country's cyber capabilities, serving as a soft power tool to demonstrate technological sophistication and readiness to counter cyber threats. They facilitate partnerships and talent recruitment for national defence and intelligence agencies, while also aiding in understanding the evolving nature of global cyber threats. Additionally, strong performance in these competitions enhances a country's reputation in cybersecurity, attracting foreign investment and stimulating the growth of the domestic cybersecurity industry. Moreover, international CTFs are crucial for educational purposes, providing practical, hands-on experience and identifying gaps in current cybersecurity education and training.

National and international CTF competitions play a vital role in demonstrating a country's cybersecurity capabilities. Success in these arenas can bolster national defence, enhance a country's standing in international relations, and contribute significantly to the growth of its cybersecurity industry and services export.

For these reasons, it is of critical importance to ensure that the individuals selected for Team UK have been assessed appropriately, and possess the suitable knowledge, skills, capabilities, and ability to be trained for competition.

SANS proposes to leverage its Cyber Ranges for the large cyber competition, focusing on practical hands-on cybersecurity training. These ranges offer participants a curated and isolated environment to apply learned skills, gaining insights into areas of strength and areas needing improvement. Participants gain real-world experience in handling cybersecurity situations without the risk associated with live production systems. This preparation equips practitioners to effectively address emerging threats and exploits upon returning to their workplaces, leveraging SANS' trusted expertise to stay ahead of evolving cybersecurity challenges.

SANS ranges are used by almost everyone who competes in face to face competitions or attends training and community events within the Cyber Security community. 'Learn, Practice, Apply' is the ideal and idea behind all ranges SANS produces, as the practical side of learning cyber skills is almost entirely reliant on hands-on experiences. All SANS training has elements of hands-on labs and most have a CTF or friendly competition to secure and reinforce the knowledge gained during the training. We find that students and participants who engage with practical experiences such as CTFs gain far more knowledge and confidence in their skills than those who don't.

During the pandemic for example, SANS hosted multiple CTFs at no cost to individuals or organisations, to maintain engagement with the community and drive the community to communicate, share knowledge and experiences to maintain the fluid sharing of resources and data. CTFs are a great vehicle for this type of training as they provide a safe place to practice, proactively promote teamwork and improve knowledge.

CTF's are primarily based on things found in the real world, they take foundational knowledge, tools and techniques and create situations and challenges which make the participant think. [redacted]

Upon award of the contract, SANS would utilise this insight and understanding to tailor the delivery of the large cyber competition and the Team UK cybersecurity training to ensure readiness to not only compete but to be successful at international competitions.

Selection of Team UK

SANS will utilise the data and analysis collected from the warm-up, semi-final, and in-person final rounds to inform the selection of Team UK. Realistically, any of the participants who were selected for the in-person final round could be considered suitable as one of the overall top 50 participants. However, to ensure that the UK can boast a winning CTF Team, selection will involve a strategic combination of talent acquisition, skill development, team dynamics, and continuous learning. SANS will utilise the following steps to build and maintain a successful CTF team:

1. Look for individuals with a range of skills including, but not limited to, network security, cryptography, web application security, binary exploitation, reverse engineering, and digital forensics. Dependent on the CTF the team are competing in, this approach will ensure a broad range of skills are present.
2. The team must be diverse in terms of skills and experience; experienced individuals bring stability, technical skill, and the ability to mentor other members, whereas newcomers bring fresh perspectives and new ideas to solve problems. This is why it is important to consider progress throughout the competition as opposed to skill level in isolation. This also generates flexibility for workload management.
3. The team will require good team dynamics and members that will promote a knowledge sharing culture amongst themselves and be supportive of their teammates to achieve shared goals.

Skills and capacity development

Once the team has been selected, they must be carefully managed and trained to ensure readiness for competition. The following will form the training and development each of the 50 team members will participate in:

1. **Continuous Learning and Training:** Team members will attend regular practice sessions to solve CTF challenges together. Regular participation together is critical, starting with smaller, local competitions and gradually moving onto larger, international competitions. After each competition, thorough analysis will be conducted to identify what went well and where improvements can be made. The team will review solutions to challenges together that couldn’t be solved with a focus on learning objectives to fill any gaps. Training will be informed by relevant CTF competitions that the team is likely to compete in to ensure team members understand the structure of the competitions and typical challenge styles. Sponsor and key partners will also input into this training allowing team members to meet with potential employers and learn how cybersecurity affects various sectors and organisations. The focus of the training will be explored in further detail in the response to Q5.

2. **Fostering Strong Team Dynamics:** The team must be able to communicate effectively with each other during competitions in order to win. This means utilising channels that will allow them to communicate during competitions such as Slack or Discord and ensuring that all team members understand their roles and when they need to communicate with each other to receive and offer support. Some team members may be more skilled in attack strategies whereas others excel in defence; understanding these roles and establishing a coordinator of resources will ensure skills are best placed during competitions. Team bonding will be encouraged through social activities and group discussions. This will mostly be facilitated virtually, as the geography of the team is likely to be widespread. However, on the occasions that the team meet in-person, SANS will arrange for social and team-bonding activities. Some of these activities will also be physical in nature to help to promote health and well-being within the team, ensuring individuals take suitable breaks from working at the computer. Creating a cohesive team will be more effective in high-pressure situations.
3. **Creating a Knowledge-Sharing Culture:** Workshops and training sessions will allow team members to share knowledge and techniques with each other without fear of judgment or asking ‘silly questions’. These sessions will also allow SANS and key partners to keep the team updated on the latest cybersecurity trends, tools, and technologies that may present themselves in competition. For team members new to the industry or seeking to gain employment, relevant courses, certifications, and pathways will be signposted.

4. **Developing and Upholding Team Values:** The team will be able to choose and develop their own team values they’d like to uphold. This will ensure each member feels a part of the team, they put the interests of the team first and treat each other fairly and with respect. This will boost team morale and promote healthy relationships.
5. **Investing in Resources:** The variety of CTF competitions will mean differences in question styles, platforms, and winning strategies. Ensuring the team has access to the necessary hardware and software tools to practice and compete effectively will be essential. Using online platforms that differ to those offered by SANS, such as Hack The Box, CTFtime, or OverTheWire will provide exposure to new challenges and allow for further practice and skill development.
6. **Developing Problem-Solving Skills:** In CTF challenges, unconventional thinking sometimes leads to solutions and encouraging team members to think outside of the box will be beneficial. Team members must also understand that CTF challenges consist of workload that has to be managed, with time needing to be monitored closely. Knowing when to move onto another challenge or crucially, ask for help, will be key.
7. **Preparing for different styles of CTF:** Not all CTFs are question-based. The team may also be required to compete in ‘jeopardy’ style CTFs, where questions are categorised and subsequent challenges are locked until previous challenges are completed, ‘defend the castle’ style CTFs, where one team must act to defend a network and systems, whilst the opposing team must try to attack that very same system, or mixed CTFs, where both of these challenge styles are

present. Providing exposure to all CTF styles will ensure the team are prepared for all eventualities.

8. **Seeking Sponsorship and Support:** Sponsorship will be sought from educational institutions, tech companies, and cybersecurity firms to provide financial support and access to better resources. Establishing a team brand, logo, and team name will also ensure that the team feel part of a community, helping hugely with engagement and commitment.
9. **Maintaining Physical and Mental Health:** Emphasising the importance of physical and mental health and ensuring the team understand the benefits of exercise, nutrition, sleep, and positive mental health can have on their overall health and performance.

Team Management

In addition to the above, the team will also require nurturing and mentorship to ensure retention and development. A critical element that will contribute to the team's success in competitions will be identifying strengths and optimising the team for participation in specific competitions. The team will understand that they can all contribute to the success of the team and some strengths may be required over others for specific competitions. The team will need to be motivated and inspired to continue, with strong performances in competitions acting as a good motivator.

Competing in Cyber Friendlies and International Competitions

Team UK will be highly skilled and will be well-rounded for participation in a range of competitions. Extensive analysis following practice sessions and local competitions will ensure the team are performing at a suitable level for entry into larger competitions. This will help to build confidence and keep team morale high. Funding from sponsorship permitting, SANS would also seek to take team members to competitions using other styles of CTF challenge to provide first-hand experience.

Post Programme

To ensure longevity of the team, sponsorship funds and buy-in from industry partners will be critical. Extensive support will have been made available for the team and this will need to continue to maintain high performance and to ensure that the UK can continue to reap the benefits this brings; the opportunity to be seen as world leaders and export opportunities for cybersecurity services. Part of this ongoing support will also need to ensure that the team is sufficiently replenished once team members age out or are no longer able to participate. SANS would seek to build plans to ensure the team can continue to grow and thrive, by holding competitions in follow-up years to select new team members.

Safeguarding

SANS is committed to ensuring the safeguarding of all participants throughout the entire lifecycle of the programme, including any online or in-person activities. This commitment begins with relevant safeguarding training. Additionally, robust safeguarding policies and procedures will be implemented and communicated clearly to all stakeholders, outlining expected behaviours, reporting mechanisms, and escalation pathways. These policies will be regularly reviewed and updated to ensure compliance with the latest safeguarding standards and regulations.

Throughout any online activities, stringent measures will be in place to protect participants' privacy and security. This includes using secure platforms with encryption protocols, implementing access controls and authentication measures, and monitoring for any suspicious or inappropriate behaviour. Furthermore, participants will be provided with clear guidelines on online conduct, including how to report any concerns or incidents. During in-person activities, designated safeguarding officers will be present to oversee proceedings and provide support and assistance as needed. Regular risk assessments will also be conducted to identify and mitigate any potential risks or hazards to participants' safety and wellbeing. By prioritising safeguarding at every stage, SANS aims to create a safe and inclusive environment where participants can fully engage and benefit from the programme's activities.

Threat management

SANS prides itself on the stringent protections that have been implemented to reduce the risk of security threats as well as the measures that will allow us to identify and respond to security incidents quickly and appropriately. Furthermore, as leaders in the training on current threats and tools such as SQL injection, XSS, and so on, we ensure all our own systems are resilient to threats of this nature, with robust and continual systems and independent penetration testing.

Ensuring user privacy and security is our number one consideration when students choose SANS. We constantly review our systems and approaches to both the security and the design of our courses and programmes and continue to adapt to and include new technologies and processes where benefit is identified. We use Open Standards where appropriate to ensure our programme delivery can occur on the maximum number of platforms and devices, whilst obeying the best of technology standards. Collection, processing, and reporting of data will be in accordance with GDPR to ensure participants understand how their data is being used.

Section Four: Delivery of Large Cyber Competition

Analysis and consideration of global cyber competition landscape and requirements

As stated in the response to Q3, SANS is uniquely qualified to undertake this project, given our extensive expertise in the global cybersecurity landscape. The project's impact extends beyond producing a winning CTF team. It aims to raise awareness of cybersecurity careers, nurture talent, and address the skills gaps facing nearly half of UK businesses. By enabling talented individuals to compete internationally, the project demonstrates the UK's commitment to addressing common threats and sharing knowledge. Success in these competitions enhances the UK's reputation as a cybersecurity leader, attracting foreign investment and facilitating the export of cybersecurity services and technologies. Therefore, selecting the right individuals for Team UK and adequately preparing them for competition is crucial.

The key elements of the large cyber competition are outlined below, along with SANS' plans for designing and delivering them in collaboration with key partners.

Competition content development

SANS are proposing a 'ladder' championship that will assess a variety of skills and disciplines in participants, providing rich data and analytics which can be used to select the team. The proposed approach utilises existing content and challenges owned by SANS which will be complemented by bespoke content and modified following feedback and insight from industry and academic partners.

As outlined in the included flow chart, the competition will start with the BootUp! CTF to ensure accessibility for all participants. The semi-final round will utilise the NetWars CTF with challenges of increased difficulty. The final round is proposed as a team-based challenge so that individuals can begin building relationships with potential future teammates and SANS can assess strengths and areas to tailor the team training.

Beginner Level CTFs: SANS BootUp! CTF range caters to beginners in the CTF domain, offering easy accessibility and a multi-disciplinary approach to cyber skills. With over 125 challenges, the BootUp! series guides players from beginner to advanced levels using hints and explainers. Participants can play solo or as a team, remotely, and at their own pace, without requiring a specialist operating system, although some opt to use one.

Intermediate Level CTFs: NetWars, SANS premier Cyber Range, offers multifaceted challenges across five levels of increasing difficulty suitable for all skill levels. Participants can tackle challenges individually or as a team, with an automated hint system available for assistance. The levels range from beginner to elite, catering to various levels of expertise in the cybersecurity field. NetWars is available in different 'flavours' tailored to specific disciplines, including multi-disciplinary events like NetWars Core, incident response-focused NetWars Cyber Defence, and forensics-oriented NetWars DFIR (Digital Forensics and Incident Response).

Advanced Level CTFs: NetWars Elite ranges, like 'Jupiter Rockets' and 'TelNet' offer advanced-level CTF experiences simulating real-life scenarios. For instance, 'Jupiter Rockets' immerses participants in a fictional rocket transport company's environment, featuring a full DMZ, internal network, and development setup. Participants must navigate through various challenges to access encrypted vaults. Similarly, the 'TelNet' range mirrors a Television News organisation, presenting diverse levels, difficulties, and technologies, including web applications, mobile apps, and malware. These simulations were featured in events like CyberThreat 2023 and the US Services Cup in December 2023.

Industry partners with technical expertise, including groups like the [redacted], will be invited to demo platforms or attempt challenges to provide feedback. They'll assess challenge breadth, difficulty, and ladder competition impact on motivation. This allows SANS to refine the competition model and gather 'dummy data' for pre-launch assessment. Partners offering cybersecurity services will contribute to the rationale for selecting Team UK, ensuring a fair and transparent process. A proposed weighting system will be reviewed by industry partners for input.

SANS highlighted in response to Q3 the formula for team readiness, emphasising collaborative training. Academic partners and technical organisations will offer complementary training for a well-rounded skillset. SANS may engage non-cybersecurity providers, such as universities offering logic and problem-solving sessions, to enhance team performance.

Hosting/platform

SANS operates in full compliance with GDPR, the Data Protection Act 2018, and UK laws and regulations and has achieved the Cyber Essentials Plus and ISO27001 certifications.

All of SANS Cyber Ranges are accessible via a dedicated platform, ranges.io (RIO), owned and operated by SANS. RIO is the front end platform supporting all cyber ranges and CTF's. It complies or is working towards compliance with WCAG 2.0. All of SANS' ranges boast a data set of participants scores, points and achievements which allows the tracking of progress and identification of where participants require focus to improve skills.

Each challenge is tagged with information about the Tools or Techniques required to solve them, which is also used to generate reports on capability, knowledge, and aptitude.

As outlined in the response to Q3, stringent protections have been implemented to reduce the risk and impact of security threats which can be identified and responded to quickly and appropriately.

User privacy will be maintained at all times; data used to access the CTF Ranges will not be shared with other participants and users will not be able to communicate with each other through the CTF Range platform ranges.io.

Dedicated online channels will be created to allow for communication between participants and other stakeholders. All users of such platform will be required to opt into a code of conduct outlining expected behaviour with clear consequences to be implemented should any user not meet those requirements. Members of the SANS team will be present in all online communities to monitor discussion and flag inappropriate behaviour.

Team UK formation/awards

Measuring an individual's cybersecurity proficiency involves assessing their current abilities in identifying vulnerabilities, understanding security protocols, and using cybersecurity tools. Conversely, measuring aptitude evaluates their potential to learn and succeed in cybersecurity roles, focusing on cognitive abilities and problem-solving skills. SANS utilises standardised assessments like CTF ranges for core knowledge evaluation and specially designed challenges with hints and explainers for aptitude assessment. Combined with in-person training and dedicated tools like the CyberTalent Enhanced Aptitude Assessment, this approach identifies core knowledge, aptitude, and the speed of skill acquisition.

Ranges.io capture metrics and data about player performance and combined with assessment tools from the SANS product catalogues establishes an overall picture of aptitude and ability, which can be improved with specific training and hands on practical exercise with qualified experts and instructors.

Once the team has been selected, SANS will host a virtual ceremony to congratulate the successful individuals and recognise their achievement to date.

[redacted] have over 17 years' experience in designing and delivering collective training support with the development of the team's soft skills and ensuring lessons learned from training and technical practice sessions are fully embedded. [redacted] have extensive Cyber and ex-military expertise within their workforce who have mentored and developed young subordinates into capable individuals and strong Cyber teams.

Competition/event management

SANS will provide technical staff for both online and in-person events to maintain a competitive 'e-sports' style atmosphere and address technical issues promptly. In-person finals will feature a dedicated network for secure access to challenges and tools. The Event Management team will handle venue setup, participant registration, and AV requirements.

Participant Engagement, Registration, Management, and Retention

The [redacted] (aged 18-25s) will form a Youth Advisory Group who will be consulted as an advisory group to ensure that plans to engage with 18-25 year olds are suitable.

SANS' existing platform ranges.io (RIO) is used as the front end to access SANS Cyber Ranges and can handle up to [redacted]. The advisory group will be asked to test the platform registration process to ensure it is user friendly and accessible for neurodivergent individuals or those with disabilities.

The Youth Advisory Group will be consulted on the competition format, incentives, and industry support. They will suggest participation incentives and ways industry partners can contribute. Feedback will be sought on access to industry events and resources. Additionally, suggestions on communication channels and preferred information types will be welcomed.

Communications and Marketing

The SANS Marketing Team will identify, with the support of the target audience, the motivations and incentives for entering the competition, to build creative messaging. Young people will also be critical in identifying the platforms and channels that the programme can be promoted through to maximise reach and engagement. The team will also build out a plan for regular communication with participants following the warm-up round to highlight strong performance and encourage returners to the subsequent stages. The programme will also require a strong brand that young people will want to be a part of and so the Youth Advisory Group will be consulted on ideas for programme names, messaging, and logos.

Industry and Academia engagement, support, and sponsorship

As outlined in the response to Q3, key partners will form an Industry Advisory Panel to oversee and provide feedback on all aspects of programme delivery. In partnership with industry and academia, SANS will develop the content for the programme through a collaborative and inclusive approach. This partnership will involve leveraging the expertise and insights of industry professionals and academic experts to ensure the content is relevant, up-to-date, and aligned with industry best practices and academic standards.

The Industry and Partnership Manager and the Industry Advisory Panel will develop a sponsorship package of options to ensure that the options are costed appropriately and will be sufficient to incentivise participation and buy-in. Options will be provided for industry and academia to contribute their own training material, allowing for diverse perspectives and innovative approaches to be incorporated into the programme. This collaborative content development process will involve regular consultation, feedback loops, and co-creation sessions to ensure that the training material meets the needs and expectations of all stakeholders. By harnessing the collective knowledge and expertise of industry and academia, SANS aims to deliver a comprehensive and impactful training programme that prepares participants for success on the global competition stage.

Monitoring, evaluation, and learning

Through the various mechanisms outlined in Q3, SANS will review feedback from key partners, participants, and DSIT through stakeholder surveys, informal feedback and group discussions and will welcome input from the Industry Advisory Panel on other suitable methods for obtaining feedback. The panel will also be consulted on the format for reviewing and agreeing suggested changes based on feedback, including how quickly these should be reviewed and changes implemented.

The Industry Advisory Panel and other key stakeholders will be able to input into project records available via secure, online platforms to ensure that data is readily available and accurate at all times, as well as the 'lessons learned' log allowing for identifiable or anonymous feedback with recommended and agreed actions communicated.

Drawing upon experience in executing similar CTF competitions across diverse global markets, SANS will apply valuable insights to enhance the monitoring, evaluation, and learning processes for this project. By leveraging lessons learned from past competitions, SANS will refine strategies, identify best practices, and anticipate potential challenges, thus ensuring the efficient and effective implementation of the project. This extensive experience will inform the development of robust monitoring and evaluation frameworks tailored to the unique requirements of the programme, facilitating continuous improvement and optimisation throughout its lifecycle.

Section Five: Delivery of training for skills and capacity development

Design and delivery of technical and general skills and capacity needs assessment

SANS will employ various elements to select participants for Team UK, including performance data from:

- The BootUp!, NetWars, and In-Person Final CTFs.
- ○ Overall rank, CTF scores, hints used, progression.
- Skills within multiple disciplines of cybersecurity.
- Previous experience and knowledge.
- Cybersecurity Aptitude
- Team-working skills.

Additionally, participants may be invited to complete the SANS CyberTalent Enhanced Aptitude Assessment to predict their aptitude towards cybersecurity principles and determine existing skill levels in domains such as Networking, Defence in Depth, and Operating Systems Security. Consulting the Industry Advisory Panel will ensure any additional requirements for team selection are considered, while seeking feedback on implementing a fair and transparent process. This competitive approach aims to select the most suitable candidates and provide a clear rationale for selection decisions, preventing discouragement and maintaining engagement in cyber activities for all participants.

Development of a training plan and strategy

SANS will design a comprehensive training programme for Team UK consisting of:

Regular practice sessions using content from SANS and other providers.

Team Building and other soft skills.

Participation in local cyber competitions.

Insight into National and International CTF competitions.

Understanding CTF roles and communication strategies.

Interactive hands-on workshops to develop technical skills.

Techniques and tool practice

Health and well-being training

Knowledge sharing and latest trends workshops.

Problem solving, workload, and time management.

Regular virtual training sessions will be conducted alongside in-person sessions at selected locations to facilitate team interaction with minimal travel, leveraging support from Universities and industry partners to host.

Depending on the skills gaps within the team, SANS may look to provide specialised training to specific members of the team, which deliberately challenge them to work on areas of weakness, encouraging them to rely on team working and communication skills to assign roles and develop a strategy to tackle the challenges.

Development of multi-disciplinary training content and material

The development of multi-disciplinary training content and materials by SANS will involve refining the plan after selecting the team and identifying their strengths and skills gaps. Collaboration with partners and input from the Industry Advisory Panel will ensure a comprehensive training plan offering exposure to various tools, products, and industry representatives. Feedback from industry stakeholders, including insights from local competitions and external content, will inform tailored training sessions. Leveraging SANS' extensive training curricula, the aim is to provide high-quality, tailored training content at no additional cost, empowering participants to excel in competitions.

With access to the largest and most comprehensive collection of training resources globally, SANS is uniquely positioned to deliver high-quality, tailored training content that addresses identified gaps and empowers participants to win at competitions.

SANS' intended partners, [redacted] will be critical in ensuring that the team members can access diverse training portfolio content. [redacted] will deliver interactive and hands-on workshops to help the team to develop their technical skills in their practice sessions; developed using their extensive expertise in penetration testing and incident response and will be able to provide focussed training in these areas.

[redacted] could provide valuable insight into the learnings captured through team training and practice sessions, supporting SANS to deliver post-event debriefs which take the trainers' and team members feedback into consideration. Post-event reports will be produced by SANS, outlining the actionable steps needed to ensure that learnings are fully understood, and improvements are implemented. This also provides focus for follow-up sessions, with reviews of previous learnings and positive improvements implemented since.

Industry partners and academia will contribute to knowledge-sharing workshops, focusing on unique challenges in sectors like banking and finance or defence, ensuring timely coverage of relevant events for the team. Developers of common cybersecurity tools will sponsor the team, providing access and running demo sessions. For instance, [redacted] delivering training on its usage, which is suitable even for beginners. Industry presence at the final round will enable engagement with participants, providing critical feedback to inform the training plan based on their performance.

Delivery of training, coaching, mentoring

SANS and our partners will also work collaboratively to ensure that team members have access to appropriate coaching and mentoring. All three organisations have experience working closely with individuals and organisations to assess skills gaps and needs and implementing tailored plans for improvement, as well as supporting individuals with additional needs. Neurodiverse individuals in particular will require additional support to ensure that they can fully access all aspects of the project, which could include more tailored support on communication and social interaction, and identifying how their skills work to complement the remainder of the team. SANS will also seek out other organisations to provide mentorship to the team, offering guidance and again, maximising their exposure to a range of diverse practitioners and sectors.

Well-being Strategy

SANS will collaborate with the Industry Advisory Panel and Youth Advisory Panel to establish a dedicated sub-group tasked with designing, implementing, and reviewing a well-being strategy. This strategy aims to define project values, promote positive relationships, and raise awareness about mental and physical health. Engagement with relevant organisations and charities will further support the well-being of the team and project stakeholders, covering areas such as mental health, neurodiversity support, and physical activity.

The sub-group will gather feedback from stakeholders to shape the strategy and initiatives, including input on desired health and well-being initiatives and the development of fostering values. Following stakeholder input, an implementation plan with methods for continuous review and feedback collection will be devised. The sub-group will liaise with the Industry and Youth Advisory Panels to ensure alignment with project goals of improving overall physical and mental well-being. SANS will oversee data collection and feedback aggregation to measure change, with regular updates shared with stakeholders and external evaluators. Upon project completion, SANS will collaborate with the sub-group to evaluate the strategy's implementation, outcomes, and impact, contributing to the wider project evaluation report.

Section Six: Experience and plans for working with youth

Project plan for key target groups

Participants in this programme will benefit from signposting to pathways, employment opportunities, and educational resources in cybersecurity. SANS offers a wealth of free online resources across various mediums. Industry and academic partners will contribute relevant inputs, including guidance from the [redacted], and networking opportunities from recognised Cyber Clusters. Signposting will occur through social channels, email, dedicated programme pages, and events.

SANS will collaborate with industry partners to keep participants engaged between CTF rounds or for those not progressing. These events will feature insights from cyber practitioners, offering guidance and networking opportunities. Team UK members will engage with cybersecurity organisations through training sessions and workshops, gaining insight into current threats and trends. They'll also access an online jobs board for suitable training and educational opportunities. Virtual events will facilitate connections with organisations offering employment opportunities. Industry representatives will provide mentorship and coaching, aiding in the development of soft skills and employability prospects for team members.

Capacities, opportunities, motivation for behaviour change (including incentivisation)

Motivation and incentivisation for behaviour change will begin with the project's outreach efforts, highlighting benefits such as free CTF rounds, networking opportunities, and access to cybersecurity experts. 'Teaser' challenges attract participants, while ladder championship progression encourages ongoing engagement. Exclusive in-person finals will be a significant motivator, offering unique networking and learning opportunities.

SANS will foster a sense of belonging among participants by facilitating introductions and building relationships with team members, industry partners, and mentors. Employing engaging learning models and gamification elements, such as digital badges and online communities, SANS aims to maintain high levels of participation. Interactive workshops will provide insights into cybersecurity careers and industry challenges.

Overall, SANS will employ a multifaceted approach to motivate participants, combining engaging content, networking opportunities, and supportive mentorship to foster a positive and enriching experience for all involved.

After team selection, SANS will ensure integration by introducing participants to the team, industry, and academic partners at in-person training events, fostering immediate relationship-building. This connection will make the opportunity more tangible, motivating participants to engage fully. Robust relationships between team members, mentors, and coaches will be established to provide ongoing support and motivation, fostering a positive team culture.

SANS has a proven track record in incentivising youth participation, demonstrated through the Cyber Discovery programme (2017-2021), engaging over 100,000 participants aged 13-18. The gamified approach sparked significant interest, with participants driven by challenges and peer recognition. [redacted]

[redacted]

Addressing the challenge of conveying the excitement and relevance of cybersecurity, the programme utilised innovative incentives and engaging narratives. Over 200 'hacking labs' provided hands-on simulations, earning participants points and badges, fostering a sense of accomplishment and community. Workshops, attended by over 3,500 young people, provided insights into cybersecurity challenges and career opportunities in the field.

Understanding the needs and engagement of youth from deprived and under-represented groups/communities (including neuro-divergent)

SANS has a strong track record of tailoring strategies and solutions to meet the specific needs of various organisations, governments, and academic institutions. This includes adapting existing knowledge and expertise to suit specific audiences, as demonstrated through initiatives like the Cyber Discovery programme.

In this programme, SANS collaborated closely with individuals, their parents, and teachers to ensure appropriate support for attendance at in-person training events and access to all training components. Staff with expertise in working with young people with special educational needs and disabilities were recruited to accompany participants, following customised support plans agreed upon by participants and their parents. These plans ensured safeguarding measures were in place while also accommodating individual needs, such as one-on-one support.

In delivering this project, establishing a diverse Youth Advisory Panel is crucial for understanding the specific needs of all participants to ensure equitable access and participation. SANS and our partners must address challenges faced by different groups, including physical access barriers for neurodiverse individuals or those with disabilities. We'll also consider stereotypes in campaign messaging to avoid alienating specific groups and work with industry to secure sponsorships for a hardship fund, aiding those facing financial barriers.

Feedback from underrepresented groups gathered through the Youth Advisory Panel will inform the programme's delivery plan to prevent discrimination. Various teams, including the SANS Pastoral Care, Industry and Partnerships, Event, CTF Ranges, Programmes, Marketing, Advisory teams, and technical and theoretical training partners, will support individuals from deprived and underrepresented backgrounds to ensure their participation and success.

SANS has collaborated with various organisations across different regions, [redacted], to deliver young adult hands-on technical training and educational initiatives. Such initiatives included a multi-step cybersecurity journey aimed at empowering underrepresented student groups, offering formalised training opportunities and unique pathways for cybersecurity education and career readiness.

Youth consultation, engagement, management, and retention

In scoping the full solution for assessing, selecting, and developing Team UK, SANS will work closely with industry and academic partners, and young people to ensure that the messaging is effective to recruit young people and keep them engaged. This will also apply to the content used in the CTF rounds for assessment, and the training to prepare the team for competitions are all suitable. [redacted] Where necessary, SANS can tailor existing content and 'off the shelf' products to maximise engagement and impact.

Section Seven: Key Stakeholder Engagement

SANS have extensive experience in establishing and maintaining lasting relationships with partners from industry, academia, and cybersecurity networks.

Previous experience in successfully engaging industry and academia

Since 2022, SANS have delivered the Upskill in Cyber programme on behalf of UK Government, engaging with over 150 organisations. SANS will look to leverage and strengthen our relationships with these existing partners, as well as continuing to build relationships with new industry partners to meet these goals, utilising a multi-pronged approach.

The SANS Marketing team will develop a comprehensive campaign to promote and raise awareness of the programme, including flyers, social media content, email sends, press articles, and partnerships with third party media. The activity will direct industry to a dedicated landing page to find out more about the programme, and ways that they can get involved.

Consultation, engagement, and retention plan

SANS have already engaged key academic and industry partners for their input on the proposed solution and to support with delivery, as outlined below. [redacted]

SANS will engage industry further through virtual webinars to explain programme aims and benefits, followed by dedicated support from an Industry and Partnership Manager to address specific requirements and solutions, including sponsorship funding.

SANS has a history of collaborating with academia, evident in programmes like the customised training and Cardiff University CTF for young adults. Additionally, SANS has provided enrichment opportunities for participants in various programmes. For instance, the top 300 participants of the Cyber Discovery programme attended in-person camps at University of Birmingham, Lancaster University, and the University of Westminster. These camps, hosted at Academic Centres of Excellence for Cybersecurity, offered formalised training, certification, and insightful panel events with cybersecurity experts, enhancing participants' skills and knowledge in cybersecurity.

SANS will implement a strategy to ensure that the delivery of this project will be beneficial to industry and academic partners, encouraging their continued engagement, not just for the initial 12 months but beyond (see Q3, Q4).

Support from industry and academia will be secured by emphasising:

- Involvement in shaping and nurturing Team UK.
- Opportunities for recognition as programme partners and supporters of Team UK.
- Understanding the wider implications of fostering a successful CTF team for the UK's reputation and the industry's growth.

Their feedback on selection criteria and processes will be vital for fostering engagement from industry and academia, ensuring the team's sustainability, and maximizing benefits for the UK.

[redacted]

Some of the ways in which industry will be engaged in this programme are listed below:

- Mentorship.
- Support with employability and sourcing opportunities.
- Team training.
- Professional development (by participating in the CTF rounds).
- Sponsorship
- Highlighting academic pathways.

Ensuring the team's longevity and project success relies on continuous industry feedback, sponsorship funds, and support from industry partners. Regularly seeking industry input and implementing improvements throughout the programme ensures adaptability and relevance. Formal reviews at project completion will capture valuable insights, facilitating ongoing team support and replenishment plans.

Project partners and support sought/secured

SANS will seek to recruit a minimum of 5 partners from industry and academia to sit on the Industry Advisory Panel and up to 20 young people to sit on the Youth Advisory Board who can be consulted on plans and key decisions.

SANS' sought support from [redacted] alongside SANS' sub-contracted partner [redacted] could support SANS with its incentivisation plans for participants and providing tailored training and development for Team UK.

[redacted] will offer valuable insights gained from delivering technical CTF Ranges and hands-on workshops to inform the design and delivery of pre-warm-up challenges and specific skills training for Team UK. Tailored workshops, conducted in-person for the team, will focus on addressing collective strengths and weaknesses, with a particular emphasis on developing skills where needed.

[redacted] unique offering could consist of reviewing training and practice sessions, supporting debriefs and contributing to post-event reports and action plans that set objectives for future sessions. Utilising principles gained from military experience, [redacted] could help to take Team UK from a group of high performing individuals to a high performing team.

We expect a minimum of 20 partners for mentorship, employment opportunities, educational pathways, and soft skills delivery. Financial contribution packages will be determined during the scoping exercise, aimed at covering the live final delivery, merchandise, international competition participation, and a participant hardship fund.

Stakeholders will be consulted at the following milestones (see Q3):

Potential challenges of working with project partners could include:

Challenge	Impact	Mitigation Notes

Partners offering services in kind fail to fulfil their commitments post-contract award.	Participants lack the advantages of a multi-disciplinary training approach.	Formal agreements ensure subcontracted partners commit to minimum delivery and support standards. SANS maintains reserves with comparable expertise in CTFs, ready to step in promptly if needed.
Industry and academia hold conflicting views on specific delivery elements.	Stakeholders disagree on scope and solutions, affecting engagement and retention.	The Programmes Team will carefully review all perspectives, conducting risk and impact analyses. Stakeholders will have access to this analysis to ensure full understanding and agreement on decision impacts.
Industry and academia disengage after the contract ends, neglecting further involvement in the team's development.	The team lacks sustained high performance and misses out on ongoing guidance from practitioners for training. Additionally, they lose opportunities for introductions to potential employers and educational paths.	Feedback from partners will be gathered to gauge motivation levels and assess the impact of the overall strategy for incentivising support. Partners will be informed of the importance of their input in implementing lessons learned and evaluating ongoing opportunities for their benefit.

Section Eight: Social Value – Health and Well-being

SANS' 'Method Statement'; how SANS will achieve this and ensure SANS' commitment meets the Award Criteria

Mission: SANS are committed to supporting internal staff, partners, and participants to improve their health and well-being through the delivery of this project and through the identification and implementation of suitable and measurable initiatives. These initiatives will also empower stakeholders to make their own decisions to improve their health and well-being.

Methodology: SANS would seek to establish a sub-group of the Industry Advisory and Youth Advisory Panels at the outset of the programme so that a group holds ownership of the strategy and can drive it forwards, alerting the Project Board of any issues arising and how these are being addressed. The overarching strategy to achieve this will focus on establishing values that promote a healthy working and collaborative culture, and initiatives to promote physical and mental health.

It is important to consider that goals may differ based on characteristics; females may have different health and well-being goals and needs than males, older individuals different from younger individuals, and neurodivergent individuals different from neurotypical individuals. Whilst the priority of the strategy will be to identify initiatives for improvement of health and well-being of stakeholders as a collective, SANS will aim to identify a range of needs and goals that are most important to individuals to be considered.

Establishing values for a healthy working culture

SANS will ensure that the working environment promotes resilience and individuals have strategies for managing stress. Establishing this culture will also ensure that individuals feel a sense of purpose to support the overall aims of the project and feel safe and comfortable in requesting support if they need it. This will help to ensure that individuals feel a sense of belonging and that their contribution is recognised and valued.

SANS will also aim to host a volunteer day for all programme partners and a dedicated mental health awareness session.

Initiatives to promote mental well-being could include:

- Trained staff available to provide support for neurodivergent individuals.
- Regular informal ‘coffee mornings’ for stakeholders to meet for non-work-related chats and support, allowing individuals to feel comfortable accessing help.
- Ability to provide anonymous feedback about working culture or suggestions for improvements.
- SANS staff providing pastoral support for participants – this is standard practice across all programmes being delivered, where regular ‘check-ins’ via their preferred method of communication are offered: 1:1 support and a listening ear. The team will also ensure that participants are actively engaging with each other and can turn to one another for support.
- Allowing individuals to be able to set their status in online communication channels so that they can avoid being disturbed when they aren’t working or need time to rest.
- Individuals being encouraged to set up designated working spaces that they can leave once they have finished working, to promote separation between work and rest.
- Dedicated channels for sharing images of loved pets have proven popular in other programmes SANS have delivered; in sharing common interests and taking a break from work.
- In project updates, positive achievements and shout-outs to individuals being highlighted to thank them for their contribution and promote a culture of sharing praise.
- A trained Mental Health First Aider will be assigned to the project to recognise signs of poor mental health, start an appropriate conversation, and signpost individuals to relevant support.
- Important updates and project progress being made available via an online noticeboard, allowing individuals to encourage individuals to take breaks without fear of missing out on important activities.

- Training on managing workloads to avoid feelings of being overwhelmed.
- Encouraging individuals to participate

Initiatives to promote physical well-being could include:

- A dedicated channel within the online communications platform encouraging individuals to share their well-being achievements, such as a walk in nature.
- A dedicated channel within the online communications platform encouraging individuals to share healthy and nutritious meal ideas.
- Sessions on desk yoga, meditation, and breathing techniques.
- Physical team building games to encourage gentle exercise.
- Establishing a group with a shared goal and the ability for individuals to encourage each other, e.g., a 10,000 steps per day goal with rewards for individuals who regularly meet the goal.

SANS staff also have access to the following initiatives and support options, and where possible, try to replicate for participants and partners:

- Access to counselling sessions at no cost if they feel that they would benefit from talking therapy.
- Flexible working options, allowing individuals to choose working hours that suit them and allow them to feel productive.
- Access to a health and well-being coach who can produce personalised exercise and nutrition plans.

Timed project plan and process

Use of metrics

It will be important to ensure that the initiatives implemented align with the areas in which individuals want to improve their health and well-being. This can be achieved through collecting information from relevant stakeholders about their current health and well-being and establishing goals to aim for, as well as suitable metrics to track a baseline position and improvements throughout the delivery of the project.

Where possible, quantifiable metrics will be used to measure progress, such as steps per day. However, health and well-being is largely subjective, and willing participants will be encouraged to complete short online surveys to self-evaluate their overall health, which can be replicated later in the programme to measure progress. The sub-group will review progress throughout the project and seek feedback from individuals on the chosen initiatives to ensure they are having the intended impact or if they need to be revisited to incentivise participation.

Tools/processes used to gather data

User-friendly online surveys will be used to gather data from stakeholders on their baseline health and well-being and any changes. The surveys will be used for stakeholders to assess their health and well-being at the commencement of the project and will suggest potential areas for improvement that the respondent can rank in terms of importance. Critically, follow-up surveys will allow stakeholders to identify any initiatives they have participated in, their experience of those initiatives and the perceived benefits to their health and well-being. Equally as important, stakeholders will also be able to provide feedback on initiatives that they haven't participated in and the reasons. This data will feed into the health and well-being sub-group who will be able to assess potential barriers that could be preventing individuals from accessing the initiatives. Changes and follow-up actions can then be agreed in an effort to improve take-up.

The SANS Pastoral Care team, mentors and coaches will also hold close relationships with the participants selected for the team and will have a greater insight into individual health and well-being. These teams will be able to provide anonymous feedback on the general health and well-being of participants as perceived through their interactions which can also be considered when assessing mid-term impact and required changes.

Reporting

As explained above, data and outcomes collected through online surveys and anecdotal anonymous feedback will be made available to DSIT, the Industry Advisory Panel, and external evaluators through weekly and monthly reporting, as appropriate. Quantitative data which highlights positive outcomes will be communicated to stakeholders through agreed channels, for example, once a collective milestone of 10,000,000 steps have been achieved. Sharing the successes will contribute to continued engagement and progress towards the overall aims.

Feedback and improvement & Transparency

The health and well-being sub-group will review quantitative and qualitative feedback at the agreed reporting points and will meet to discuss achievements and options for improvement. Anonymous findings will be published to stakeholders and respondents along with the advice and suggested follow-up plans developed by the sub-group. Stakeholders will have the opportunity to provide their feedback on proposed plans before any changes are implemented.

To address the policy outcome of influencing staff, suppliers, customers, and communities to support health and well-being through the contract, a comprehensive approach encompassing various aspects of social value can be adopted.

In summary, promoting community engagement and sustainability initiatives within the contract framework can foster a sense of social responsibility and environmental consciousness. This can include partnering with local organisations for community projects, implementing eco-friendly practices, and supporting sustainable sourcing from suppliers.

Furthermore, prioritising employee well-being through initiatives such as health and wellness programmes, mental health support, and work-life balance policies can contribute to a positive workplace culture and employee satisfaction. Encouraging skill development and career growth opportunities for both employees and suppliers through training programmes, mentorship, and capacity-building initiatives can empower individuals and promote upward mobility.

Additionally, emphasising ethical practices throughout the supply chain and encouraging volunteering activities among staff and stakeholders can further enhance the social impact of the contract. By integrating these measures into the contract delivery process, it will become possible to create a holistic approach that not only delivers on contractual objectives but also generates significant social value by levelling the playing field, fostering growth, supporting development, and promoting ethical practices.

Order Schedule 5 (Pricing Details)

Table A: Payment Schedule

Milestone and percentage of payment (Total Fixed Price)	Deliverable	Expected date	Price (excl VAT)
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
		Total	[redacted]

Table B: Rate Card

Description of Service Management & staff and their respective man-days:				**FIXED PRICE (£ excluding VAT)**
			[redacted]	
Name	[redacted]		[redacted]	
[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]			[redacted]	
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]	
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]	
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]	
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]			[redacted]	
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]			[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]			[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]		[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]				
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]			[redacted]	[redacted]
[redacted]	[redacted]	[redacted]		[redacted]
				[redacted]
[redacted]				[redacted]

Table C: Detailed Breakdown

Attached as Appendix C

Order Schedule 7 (Key Supplier Staff)

1. The Annex 1 to this Schedule lists the key roles ("**Key Roles**") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.

2. The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

3. The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

4. The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);

4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or

4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

5. The Supplier shall:

5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;

5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least 1 Months' notice;

5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and

5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.

6. The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

Annex 1- Key Roles

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Order Schedule 20 (Order Specification)

1. Introduction and summary of requirements

The Department for Science, Innovation and Technology (DSIT) is appointing the Supplier to deliver a new Cyber Skills Programme. In summary the requirement will be to:

1) establish a 'Team UK' – a group of up to 50 (minimum 30) 18–25-year-olds through a technical, competitive process; 2) ensure Team UK are trained and supported to a high, global standard, and 3) ensure Team UK successfully represents the UK at international cyber friendlies (e.g., with Team US and Team Ireland) and competitions (e.g. the International Cybersecurity Championship and European Cybersecurity Challenge).

As part of point 1, to find talented young people to join Team UK, we would like to hold a UK-wide 'capture the flag' cyber competition for interested 18–25-year-olds (participants must be no older than 25 by the end of FY 24/25). This would ideally consist of an online 'warm up' event (optional based on funding priorities) and a competitive first round (online) for a minimum of 500 participants (flexible, based on target market and availability), followed by an in-person final for a minimum of 200 finalists (flexible). The cyber competition should have an engaging and innovative format influenced by elements from 'e-sports', to ensure uniqueness and popularity.

The top 50 (minimum 30) competitors will go on to form Team UK and will then be assessed and provided bespoke training and coaching by the supplier and industry partners, sponsors engaged by the supplier for the project.

This project is at the proof-of-concept stage, and therefore any targets for competition rounds and participant demographics will be flexible. The priority is ensuring that a large and diverse group is successfully engaged to ensure 'Team UK' is highly competitive and representative of the UK.
The supplier and any partners engaged, will ensure Team UK's successful preparation and participation in international friendlies and competitions.

The above will be delivered based on a mixed, online, and in-person format conceived on the balance of available resources and the best intended quality and outcomes.

Policy Context to The Requirement

In 2022, the government published the National Cyber Strategy setting out how the UK will solidify its position as a global cyber power. DSIT is playing a key role in delivering the strategy, responsible for strengthening the UK's cyber ecosystem and ensuring the UK has a sustainable supply of home grown cyber skilled professionals to meet the growing demands of an increasingly digital economy.

Despite high demand for skilled cyber security professionals, there is a need to motivate more young people to think of cyber security as a career. The Cyber Security Labour Market Survey 2023 showed that cyber security faces a significant skills shortage, with an annual shortfall of approximately 11,200 people needed to join the workforce vs the previous year estimate of 14,000. Widening and increasing the talent pool remains key to tackling skills shortages and improving diversity. People from ethnic minority backgrounds make up 22% of the sector workforce, similar to last year's figure of 25%, and 14% of those in senior cyber roles are from ethnic minority backgrounds (i.e. those typically requiring 6 or more years of experience). 17% of the workforce are female, which is in line with findings in 2020 and 2021.

There are currently a number of cyber skills initiatives targeting the under 25s, delivered by DSIT and the National Cyber Security Centre (NCSC), which help young people engage with cyber in order to build a sustainable and diverse pipeline of cyber security talent. For example, the Cyber Girl's competition for 12–14-year-olds and Cyber Explorers, an online learning platform for 11–14-year-olds. However, DSIT does not currently have any active programmes that identify and support the development of young people with advanced cyber skills and showcase career opportunities. We are aware that cyber competitions are popular with young people and industry; competitions are often used by industry to network and recruit people with advanced cyber skills. Therefore, this project will form part of DSIT's package of youth initiatives and bring together high levels of industry engagement and cross government collaboration to address the current gap in activities around supporting top cyber talent. This project will attract young people to the cyber profession, provide opportunities for cyber skill development, provide opportunities to network with government and industry employers, and strengthen the UK's international reputation as an international cyber power.

Many governments around the world use National Cyber Security competitions to encourage young people to pursue cyber, nurture students' interest and attract talented individuals to the cyber sector[1]. Beyond that national cyber competitions are said to support with wider objectives, such as:

- Promoting diversity in the cyber sector
- Increasing interest in cyber security knowledge and skills
- Increasing interest in cyber careers and connecting participants with potential employers
- Create a network of young cyber security specialists
- Encouraging open cyber security knowledge[2].

The objectives of other national cyber competitions match DSIT policy aims. This project will complement wider government work to develop a sustainable and diverse pipeline of talent for the cyber sector.

Thirty-four countries attended the most recent European Cyber Security Challenge (ECSC), run by the European Union Agency for Cybersecurity (ENISA). At the 2023 International Cyber Challenge, there were teams representing Europe, North America, South America, Oceania, Asia and Africa. Neither competition currently has any representation from the UK. By establishing 'Team UK' to participate in these competitions and bilateral cyber friendlies, there will be opportunities for the UK government to demonstrate its commitment to cyber security on the international stage and to increase the UK's involvement in international cyber communities. The planned training programme for Team UK will ensure that UK representation has the skills and knowledge to be fully competitive and provides further opportunity for industry and government collaboration as industry sponsors can support with training events.

This programme would also seek to increase collaboration across the cyber ecosystem with cross-government, industry and academic support and engagement. The National Cyber Force (NCF), NCSC, Academic Centres of Excellence in Cyber Security Education (ACE-CSEs) and other stakeholders have expressed interest and support. The UK Cyber Competition is an opportunity for industry and government to engage with talented young people from diverse backgrounds, shape their development and showcase work placement or job opportunities. Networking and mentoring will be a key part of the programme, in order to support young people to make connections with the cyber ecosystem and develop their career.

2. The Requirement

DSIT are appointing the Supplier to deliver the following aims:

- Run a national, cyber 'capture the flag', 'e-sports' inspired competition for 18–25-year-olds to identify 50 young people (30 minimum) who will form Team UK. This competition should have two rounds, one virtual and one in-person final. Inclusion of an online warm-up round is preferable.

- Run a training programme to build the skills and knowledge of Team UK in preparation for international competitions. This training programme will be a mixture of virtual instruction-based and in-person bootcamps supported by industry sponsors, and online self-directed learning. The training programme must support the mental and physical well-being of participants.

- Have Team UK take part in international competitions and cyber friendlies against other national teams, with the aim of 3 cyber friendlies in FY 24/25.

- Build strong industry and academic partnerships and sponsorship to support the project.

Key deliverables/results:

- Successful development of high-quality project plans, strategies, structures, systems, processes, methodologies, content, and tools as may be required to ensure overall successful project planning, design, delivery, and oversight.

- Successful identification, consultation, engagement, securing, and retention of industry and academic partners and supporters for wide-ranging support (material, technical, financial, instructional, etc.), across all key functions and phases of the project (planning, design, implementation, oversight, and evaluation) ensuring successful planned outcomes/results. In addition to industry and academia support to this project and its partners, the plan would seek to build and strengthen the wider cyber eco-system.

- Develop and establish sustainable pathways/support for academic, career development and employment opportunities for members of the Team UK pool, as well as for those others who participate in the competition/project.

- Successful planning and implementation of a UK–wide Cyber Competition with warm-ups (optional), Round 1 (online), and final cyber competition (in-person) events.

- Successful identification and engagement of Team UK members/pool (A minimum of 30 and up to 50 young people within the ages of 18 to 25).

- Successful formation of Team UK, design and implementation of technical and general skills assessments, and the delivery of a tailored skills and capacity-building and training and coaching package in partnership with industry, academic, and government partners/sponsors to ensure Team UK meets the highest level of global competition standards.

- To demonstrate proof of concept, a priority for the newly formed and trained 'Team UK' in the FY24/25 (Q3/Q4 period) will be to participate in international cyber friendlies, competing (online) against other national teams such as Team US and Team Europe. We expect the Supplier to support and co-lead the successful delivery of up to 3 virtual events with DSIT. It is noted that the delivery of this is dependent on a number of variables outside the control of the Supplier.

- Successful comms and marketing campaigns designed and delivered to relevant external audiences to ensure delivery of key project aims (ensure best top-talent secured from across UK). This will have a particular emphasis on ensuring young people from under-represented and diverse backgrounds will be engaged and supported. Close collaboration with DSIT comms teams will be expected when planning and delivering comms and marketing campaigns. DSIT requires all marketing and communications activities to be signed-off by the Department ahead of delivery. For this purpose, the Department requires these to be provided in draft form with adequate time to review and feedback, and for suppliers to be able to action any creative and strategic feedback provided. The Supplier will be expected to provide verbal and written reports on marketing strategy (separate to other expected project management updates) measured against comms-specific KPIs that are to be agreed at project inception. Once the Supplier is appointed, DSIT will hold meetings to understand and agree clear marketing plans related to the programme. The Department will support marketing of the project as much as possible through our own delivery channels, where these are available.

- Successful design and delivery of monitoring, evaluation, and learning components (including project reports, learning events, etc.) ensuring critical knowledge and insights relating to the pilot project are captured and shared with key partners to support establishing a scaled, multi-year public-private programme. If this requirement is met by the Supplier (and not by an independent third-party evaluator), the supplier should demonstrate how the MEL functions, methodologies, processes, and findings are as objective as possible (e.g. ensuring multi-stakeholder inputs and oversight). As part of this, the supplier should collect and report on diversity (required disaggregation criteria will be provided by the Department). As this is a pilot project, gaining a nuanced understanding of the backgrounds and characteristics of the applicants/participants will inform future policy development, and will be a key part of the project evaluation and success. Any individual data collected as part of the project must comply with all relevant UK data protection laws and standards.

Other Requirements

- The Supplier must ensure they are compliant with Cyber Essentials. They must also demonstrate the 12 Technology Code of Principles[3]. It is a requirement that the supplier demonstrates how they plan to adhere to the 12 Technology Code of Principles in the Tender response submission. In meeting the above principles, it must be demonstrated that the digital services are resilient to publicly available tools (e.g. SQL Map, Burp Suite, Metasploit) and techniques (e.g. cross-site scripting, SQL injection, directory traversal and password stuffing). Before final acceptance of the digital services, the supplier will be required to provide evidence (at their own cost) that it meets these requirements through an independent penetration performed by a company within the NCSC's CHECK scheme. A copy of the test report shall be provided to the Authority as proof of conformance against the principles.

Project Reporting

The Supplier will be required to provide project reports periodically based on an agreed template. The format, frequency, and level of detail will be agreed with the Department in the project inception period.

Project KPI's

KPIs agreed with the Supplier includes the successful delivery of the following as a minimum:

- **Industry support**
  - Minimum of 40 industry supporters secured (15 of these being new organisations to SANS).
  - This will include £130k secured in financial contributions and an additional £150k equivalent of in-kind services.
- **Youth engagement, national competition, and formation and training of 'Team UK'**
  - Deliver a warm-up event with 1000 participants; a semi-final event with 400 participants; and a final event with 200 participants.
  - Formation of Team UK (minimum of 30 members)
  - Provision of 3 in-person tailored training events (developed based on skills and capacity needs assessment of Team UK members) together with other virtual instruction/self-learning-based learning opportunities.
- **Team UK Activation/Representation (Optional – based on additional funding being secured)**
  - Contribute to the delivery of up to 3 friendlies against non-UK cyber teams (virtual).
- **Reports and Learning**
  - Submission of two high-quality project reports (mid-term and end-term)
  - Delivery of a final review and learning event at the end of the contracted project period.

The KPIs will be reviewed and revised (including incorporating MEL and communications requirements) with the supplier in the immediate project planning and design phase (post-contract award). These KPIs are subject to future review, monitoring, and revision in agreement with the supplier, as may be required by DSIT.

Working Arrangements

It is proposed that the work be structured as follows:

Activity	Timeline	Budget (Excl. VAT)
Contract award	15th March 2024	N/A
Kick Off Meeting	18th March 2024	N/A
Project planning and design (delivery of key project plans and strategies by supplier for review – in final draft form)	March 2024	£50,000
Conduct research and finalise project plans, model, structure, etc.	FY24/25	£400,000
Secure industry partnerships and support		
Competition content development		
Comms and marketing campaign		
Participant registration		
Hold domestic competition warm up(s), Round 1 and Final		
Form Team UK and conduct technical assessments		
Team-building and technical skills development (training content design and delivery)		
Preparations and participation in international cyber friendlies and competitions		

The Department requires a robust governance and oversight function and process for this project, with close and frequent coordination, discussion, and interaction between the DSIT project managers and the supplier/partners across and throughout the project. A multi-stakeholder project board is also seen as a key requirement for project success.

Protection of information & security arrangements:

The supplier and their subcontractors will be required to sign (or abide by) a non-disclosure agreement and apply DSIT information security policies to all information they access as part of this work, including ensuring that only duly authorised personnel can access protectively marked information. The supplier and their subcontractors will need to demonstrate the availability of adequate infrastructure and a business continuity plan to deliver the work to a high level of quality at the required time, ensuring the protection of information at all times.

Period of Contract:

The contract shall run to 31 March 2025 or until the contractor satisfactorily delivers the requirement.

Price and payments:

In submitting full tenders, suppliers confirm in writing that the price offered will be held for a minimum of 60 calendar days from the date of submission. Any payment conditions applicable to the prime contractor must also be replicated with sub-contractors.

A breakdown of billable days or hours of work undertaken the previous week must be provided by the supplier promptly each week, along with the relevant invoice, to assist DSIT's cost control and payment processes.

DSIT's target is to pay all approved invoices within a maximum period of 10 days.

Department for
Energy Security
& Net Zero

Department for
Science, Innovation
& Technology

DESNZ & DSIT: Environmental Policy

DESNZ and DSIT are UK government departments respectively leading on energy security & net zero and science, innovation & technology. We are committed to protecting the environment and preventing pollution. We undertake all our activities in a responsible manner, using best practice, to reduce the environmental impacts of our operations and to enhance and improve environmental performance and the Environmental Management System. DESNZ and DSIT are committed to fulfilling all environmental compliance obligations as a minimum and will strive to continually improve the environmental performance of our buildings, operations and supply chains.

DESNZ & DSIT will:

- Proactively reduce our carbon footprint by implementing energy saving practices and technologies, to be more energy efficient;
- Mitigate the impacts of business travel through relevant policies and procedures;
- Preserve and enhance biodiversity on our sites where we have opportunities and scope to do so;
- Proactively use innovation and technology to ensure efficient use of water;
- Embed the Waste Hierarchy into all waste procedures while also managing waste according to our duty of care;
- Understand and assess climate change adaptation risks for our key sites, to ensure business continuity and resilience;
- Consider sustainability in all procurement decisions, focusing on decarbonisation, sustainable resource use and climate change adaptation;
- Minimise the consumption of natural resources and reducing environmental impacts through our supply chains;
- Manage fuels and hazardous substances appropriately to minimise environmental risks;
- Regularly review performance of environmental objectives and targets;
- Regularly report on progress to the senior responsible officer;
- Communicate this policy to our staff, to everyone working for or on behalf of DESNZ and DSIT and interested parties to ensure they understand the environmental impacts of their job and how to minimise these.

DESNZ and DSIT shall monitor and review effectiveness of this policy through ISO 14001:2015 Environmental Management System and in conjunction with the ISO 50001:2018 Energy Management System.

Endorsed and signed by:

Michael Pittams

Deputy Directorr
Estates and Sustainability, June 2023

TITLE:	DESNZ & DSIT VSP 00 ENVIRONMENTAL POLICY			ISSUE NO	1.5
REVIEWER:	Richard McAlorum	APPROVER:	Michael Pittams	ISSUE DATE:	Jun-23

HM Government

Government Functional Standard

GovS 007: Security

Version: 2.0
Date issued: 13 September 2021

Approved

This functional standard is part of a suite of management standards that promotes consistent and coherent ways of working across government, and provides a stable basis for assurance, risk management and capability improvement.

The suite of standards, and associated guidance, can be found at **GOV.UK government functional standards**.

Functional standards cross-refer to each other where needed, so can be confidently used together.

They contain both mandatory and advisory elements, described in consistent language (see the table below).

Term	Intention
shall	denotes a requirement: a mandatory element.
should	denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	denotes a description.

The meaning of words is as defined in the Shorter Oxford English Dictionary, except where defined in the Glossary in **Annex B**.

It is assumed that legal and regulatory requirements are always met.

Version 2.0 of this standard replaces the previous edition V1.0 dated July 2020. The main changes, which reflect input from users of the previous version, are as follows:

- a substantial improvement of the incident management section
- a greater inclusion of aspects of risk and threat throughout
- a stronger technical security section

Produced by Government Security Group

Contents

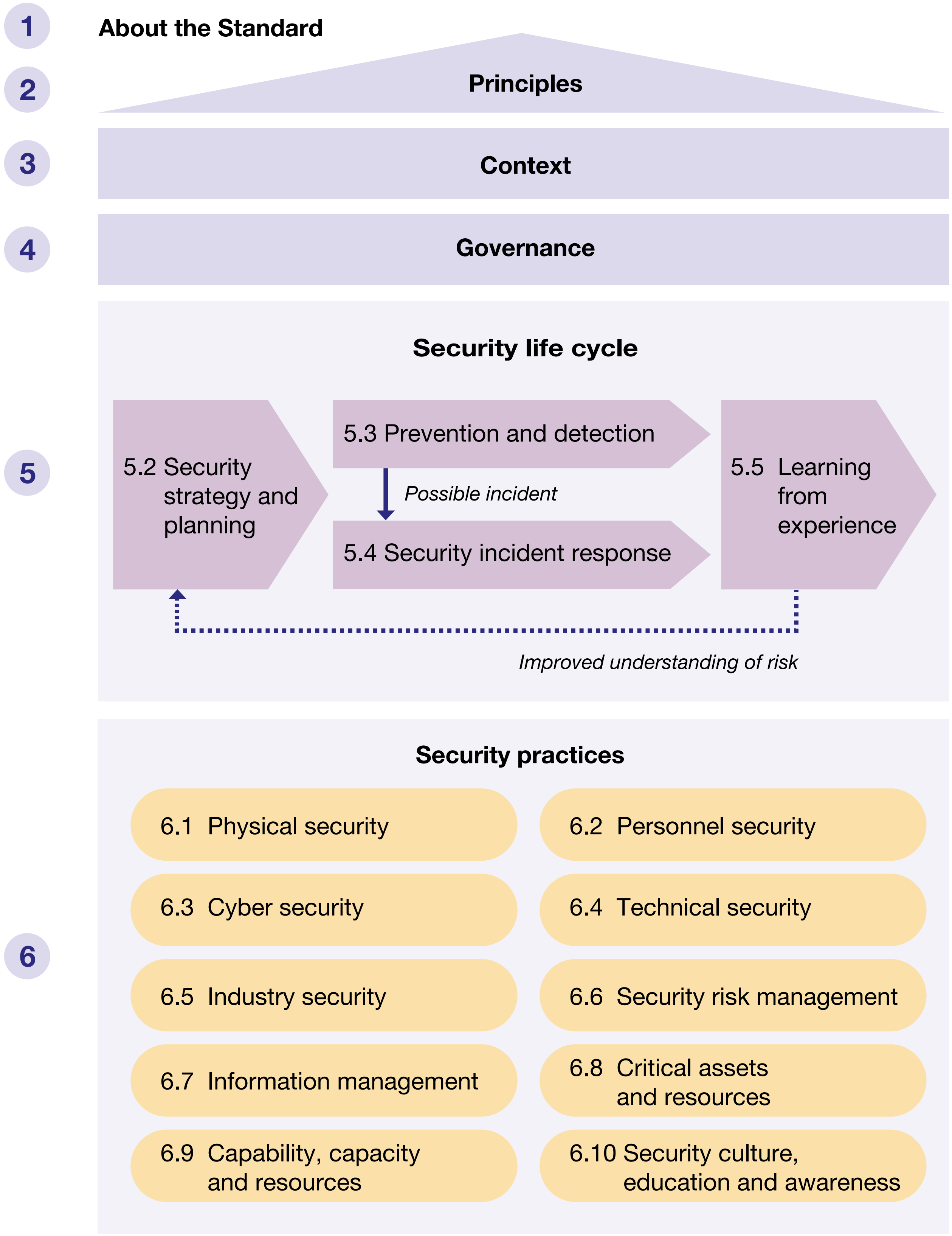

1
About the Standard
2
Principles
3
Context
4
Governance
5
Security life cycle
5.2 Security strategy and planning
5.3 Prevention and detection
Possible incident
5.4 Security incident response
5.5 Learning from experience
Improved understanding of risk
6
Security practices
6.1 Physical security
6.2 Personnel security
6.3 Cyber security
6.4 Technical security
6.5 Industry security
6.6 Security risk management
6.7 Information management
6.8 Critical assets and resources
6.9 Capability, capacity and resources
6.10 Security culture, education and awareness

Figure 1 Scope of this functional standard

1 About this government functional standard

1.1 Purpose of this government standard

The purpose of this government functional standard is to set expectations for protecting:

- the government's assets (people, property and information)
- visitors to government property, and third party suppliers whilst engaged on government business
- citizen data

This standard provides direction and guidance for:

- permanent secretaries, directors general and chief executive officers of arm's length bodies, to ensure the right environment for effective delivery and performance
- security advisers and other named security officials
- those responsible for communicating security information to government staff and visitors
- those working within and for the government, who have a responsibility to ensure security practices are followed (including staff, third party suppliers and members of the armed forces)

Note: this standard replaces the Security Policy Framework. The policies which sit within that framework remain in effect but are now in support of this standard.

1.2 Scope of this government standard

This standard applies to the planning, delivery and management of government security activities. It includes risk management, planning and response for physical, personnel, cyber and technical security in departments and their arm's length bodies, as well as industry [1 and 2]. Other public sector organisations, devolved or local, may find this standard useful.

Note: an organisation, in the context of government functional standards, is the generic term used to describe a government department, arm's length body, or any other entity that is identified as being within scope of a functional standard.

The structure of the standard is shown in Figure 1.

1.3 Government standards references

The following standards are directly necessary for the use of this standard:

- GovS 003, Human resources
- GovS 004, Property
- GovS 005, Digital, Data and Technology
- GovS 008, Commercial
- GovS 010, Analysis

A functional standard supports achievement of the outcomes sought by an organisation. It sets expectations for what needs to be done and why, relating to the functional work within its scope, in order to achieve those organisational outcomes.

Note: for expectations relating to management of a function across government and management of functional standards, please see GovS 001, Government functions.

2 Principles

Those engaged in the management of government security shall ensure:

1. security objectives are aligned to government policy and organisational objectives
2. a security risk management approach is adopted, based on an assessment of threat and vulnerability, that enables the business of government and is aligned to government policy and organisational objectives
3. security risks are managed appropriately, with governance frameworks and controls proportionate to the prevailing level of risk
4. security planning is holistic, covering all aspects including physical, personnel, cyber, technical and industry aiming to prevent incidents as well as responding and learning from them
5. protective security reflects the UK's national security objectives and protects the government's most sensitive assets
6. there is a focus on embedding the right security culture and behaviours
7. work is assigned to competent, appropriately skilled people
8. accountabilities and responsibilities are defined, mutually consistent, and traceable across all levels of management
9. public service codes of conduct and ethics as well as those of associated professions are upheld

3 Context

3.1 Introduction

This section provides essential background information for the use of this functional standard.

3.2 Overview of security

The Prime Minister is ultimately responsible for the security of HM Government. The Prime Minister delegates accountability to the Cabinet Secretary, who in turn delegates accountability to Permanent Secretaries and Accounting Officers. Accounting Officers are accountable to Parliament for the security of their organisations.

The Government Security Group oversees government security at the direction of the Government Security Board and is responsible for the development of good practice in relation to security.

The Government Security Group is distinct from the Cabinet Office's National Security Secretariat, which delivers the government's national security, foreign policy priorities and shapes the UK's response to international issues which impact national security.

Management of security is on three levels, Cross-government, Government Security Centre and Organisational (departments and arm's length bodies).

3.3 Integrated protective security

Protective security comprises four interconnected domains, through which attacks are perpetrated: physical, personnel, cyber and technical. Although they are considered as separate domains, they rarely occur in isolation and are treated holistically.

Physical security is the practice of protecting elements of government infrastructure, estates, physical assets and personnel against attacks or compromises in the physical (i.e. tangible, real-world) environment.

Personnel security is the practice of ensuring the security of government information and infrastructure against threats arising from government personnel, others working to government and those who formerly worked in HM Government circles. This could include deliberate attacks, criminal activity for profit, unmalicious and unwitting insider threat, or gross negligence, and could manifest in a variety of environments, including the physical (i.e. tangible, real-world) or virtual (i.e. in cyberspace) environments. Such individuals could join government service intending to commit such acts, or decide to do so after employment [1].

Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from the deliberate and inadvertent exploitation of computer systems, technology-dependent enterprises and networks [2].

Technical security is the practice of detecting the compromise of protective security systems, analysis and prevention of technical attack, mitigation of technology vulnerabilities and the deployment of countermeasures.

Government security also includes the protective security arrangements of industry partners that provide goods and services to government or which hold government or international partners' classified information. This is described in government security as 'industry security' (see 6.5 for more detail).

Underpinning all four is good incident management - the organisation's response to a security incident. A security incident is any circumstance that has arisen with the potential to compromise government assets including people, property or information.

4 Governance

4.1 Governance and management framework

4.1.1 Overview

Governance comprises prioritising, authorising, directing, empowering and overseeing management, as well as assuring and reviewing performance.

A governance and management framework shall be defined and established for the management of security across government as a whole, and in government organisations.

The governance and management framework should include the authority limits, roles and rules for making business decisions, degrees of autonomy, assurance needs, reporting structure, accountabilities and responsibilities, together with the appropriate management practices, processes and associated documentation needed to meet this standard.

4.1.2 Cross-government management

The cross-government governance and management framework should include cross-government security policies, to set expectations for managing security in order to protect UK government assets (people, information and property). The policy framework should focus on outcomes required to achieve a proportionate and risk-managed approach to security that enables government business to operate effectively, safely and securely.

The cross-government governance and management framework should be supported by policies, standards, best-practice guidance and approaches which should be maintained and communicated to those with organisational security responsibilities.

4.1.3 Organisational management

The governance of security-related activities within an organisation should be an integrated part of that organisation's overall governance, to align security objectives and requirements with the organisation's strategic aims and delivery objectives.

Each organisation's governance and management framework shall cover physical, personnel, cyber, incident management, technical and industry security [1 and 2].

The governance and management framework should cover the practices described in this functional standard.

Security management frameworks should be responsive to new and changing circumstances and reflect actual and emerging security threats as well as including how organisations should manage risk (see 6.6). Where systems have broken down or individuals have acted improperly, appropriate action should be taken.

The accounting officer for each organisation shall appoint:

- a board member (or equivalent) with a specific security remit (see 4.4.5)
- a senior officer accountable for security (see 4.4.6)

Organisational senior officers accountable for security should work together to ensure policies, practice guidance and processes are followed in their respective areas in order to mitigate security risk.

4.2 Assurance

The purpose of assurance is to provide, through a systematic set of actions, confidence to senior leaders and stakeholders that work is controlled and supports secure and successful delivery of policy, strategy and objectives. Organisations shall comply with mandated cross-government assurance activities as coordinated by the Cabinet Office.

4.2.1 Assurance framework

Objective, evidence-led evaluation of the effectiveness of the government's security controls should be undertaken to monitor delivery, identify activities and support improvement, and to make informed decisions. Analysis in support of evaluation shall be undertaken in accordance with GovS 010, Analysis.

Organisations should have a defined and established approach to security assurance, which should be applied proportionately to the risk and value of the activity, and integrated with the organisation's overall assurance framework. Typically, assurance should be on at least three separate and defined levels including:

- by, or on behalf of, operational management within organisations, applying judgement to support successful delivery and adherence to functional standards
- by, or on behalf of, senior management, independent of operational management, in accordance with the defined assurance approach
- by independent bodies (within or external to government, such as internal audit and National Audit Office) to provide an objective evaluation of the adequacy and effectiveness of governance, risk management and controls

The work of internal and external assurance providers should be planned to minimise disruption to other work, avoiding overlaps with other assurance activities and duplication of effort, whilst remaining rigorous and meeting the needs of stakeholders.

Where assurance includes formal review activity, the customer for the review should be clearly identified.

The requirements of the Orange Book: management of risk - principles and concepts, shall be met [3].

4.2.2 Human resources and security

Due to the interdependencies between personnel security and human resource management, organisations shall include the assurance of human resource management activities within their organisational approach to security. Human resource activity should be assured at three levels:

- first by human resource managers operating within established frameworks to the organisation's risk threshold
- second by risk, quality and compliance professionals within the organisation
- third by cross-government independent audit experts

GovS 003, Human Resources shall be followed.

4.3 Decision making

Decisions should be made and approvals given in a timely manner in accordance with the organisation's security governance and management framework (see 4.1.3). Government standards and policy should be complied with. Decisions should be made by assessing options against defined criteria and in consultation with stakeholders and subject matter experts. Decisions should relate to:

- setting policy for security across the government, security centre or organisation
- developing new controls for a perceived threat to government security
- approving plans for adhering to this security standard and associated requirements
- security vetting
- responding to events, incidents or crises

Analysis shall be undertaken in accordance with GovS 010, Analysis.

4.4 Roles and accountabilities

4.4.1 Overview

Roles and accountabilities shall be defined in the relevant governance and management framework and assigned to people with appropriate seniority, skills and experience. This should include, but is not limited to, the activities, outputs or outcomes they are responsible for, and the person they are accountable to.

Note: for more detail on roles, see also [4].

4.4.2 Senior officer accountable for security across government

This role is accountable to the Civil Service Board for cross-government security policy and standards and for advising accounting officers on setting the risk threshold for their organisations. In particular the senior accountable officer should:

- define and establish the cross-government security strategy and cross-government policy and standards
- monitor performance against policy and standards
- provide guidance and direction to the senior security role holders, when requested
- respond to serious and/or cross-government security incidents or issues
- define the groups of organisations for which coordinated management of security is necessary (see 4.4.3)

Note: this role also leads the Security function across government and is currently known as the Government Chief Security Officer.

4.4.3 UK National Technical Authorities

Organisations draw on expert advice and support in the four domains of security from the UK National Technical Authorities: the Centre for the Protection of National Infrastructure on physical and personnel security; the National Cyber Security Centre on cyber security; and UK National Counter-Eavesdropping on technical security.

Note: defined groups of organisations clustered together for security management are known as Government Security Centres.

4.4.4 Accounting officer

The permanent head of a government department is usually its Principal Accounting Officer.

An organisation's Accounting Officer is accountable (via a Principal Accounting Officer where appropriate) to Parliament and the public for the stewardship of public resources, ensuring they are used effectively in the arm's length bodies within the department's ambit as an Accounting Officer.

An Accounting Officer (or equivalent in an arm's length body) is the senior officer accountable for security in an organisation, supported by their management board.

4.4.5 Organisational board members

A board member shall be appointed by the Accounting Officer to have specific responsibility for oversight of security compliance and auditing processes, including arrangements to determine and satisfy that delivery partners, service providers and third party suppliers, apply proper security control, including understanding and managing security issues that arise because of dependencies on external suppliers or through their supply chain (see 6.5).

Each management board member in an organisation is accountable to the Accounting Officer (or equivalent in an arm's length body) for oversight of, and responsibility for security risk management in their respective business area(s).

4.4.6 Senior officer accountable for security in an organisation

This role is accountable to the Accounting Officer (or equivalent in an arm's length body) for the implementation and maintenance of security standards across the organisation and for ensuring correct procedures and delegations are in place to respond to security incidents.

They shall be responsible for:

- advising the organisation's senior officers on security issues, including the management of security risks
- ensuring an effective relationship between the organisation and those coordinating wider security provision (see 4.4.3)
- appointing an incident manager, when needed
- articulating the security needs of their organisation
- overseeing and reporting on the delivery of services to agreed standards
- defining and owning local security policies
- professional training, qualifications and continuous development
- requesting advice and guidance for the senior officer accountable for cross-government security, when needed

The senior officer accountable for security in an organisation should act as an intelligent customer, taking on responsibility for defining the security services required by their organisation, requesting services from the Government Security Centres (see 4.4.3) and ensuring the requirements of their organisation are being met to agreed standards and service level agreements.

4.4.7 Senior officer responsible for security information in an organisation

This role is accountable to the senior officer accountable for security in an organisation for:

- advising the organisation's board on how to balance the needs of security and exploitation of technology to deliver the organisation's strategic objectives, and provide strategic leadership for the organisation's cyber and information security community and its investment in security technology
- developing and maintaining the organisation's security strategy, security architecture, policies and standards, technology assurance and professionalism
- supporting the senior officer accountable for security in requesting seniors from the cyber security centre

Note: Some departments may adopt the model of the senior officer responsible for security information in an organisation being accountable to the senior officer for security or to the Accounting Officer.

4.4.8 Incident manager

The incident manager is accountable to the senior officer accountable for security in an organisation (see 4.4.6) for the management and resolution of an incident and any subsequent breach, in particular assessing:

- the type of incident
- the risk and impact to the organisational assets
- any commercial or supply chain considerations
- implementation of plans to respond to the incident
- investigating how the incident occurred and providing lessons learned

The person appointed as an incident manager should not have any conflict of interest in investigating the incident.

Note: the senior officer accountable for security in an organisation can undertake the role of incident manager. For cross-government incidents this role can be undertaken by the senior officer accountable for cross-government security.

4.4.9 Security specialists

Other specialist security roles should be defined to suit the needs of the security-related activities being undertaken. This can be for a variety of aspects of security practice in accordance with this functional standard and the organisation's governance and management framework. Such roles may be advisory or executive.

Note: examples of specialist roles include, but are not limited to, risk owners, information asset owners, data protection officers, communications security officers, crypto custodians, intelligence handling coordinators, physical security controllers, Facility Security Clearance (List X), personnel security controllers and board level contacts.

5 Security life cycle

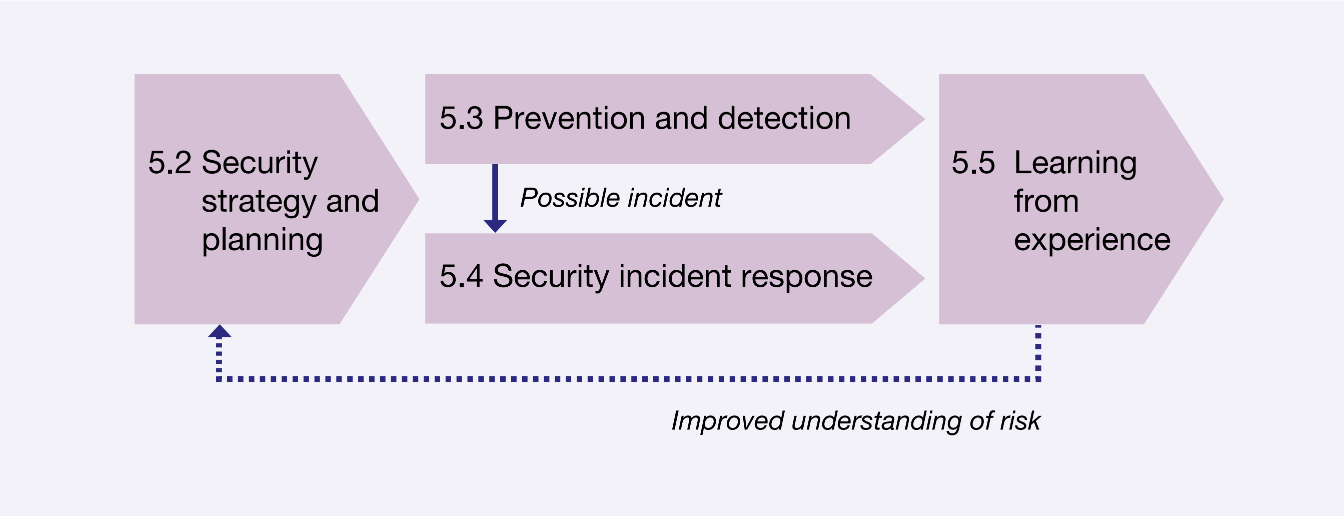

5.2 Security strategy and planning
5.3 Prevention and detection
Possible incident
5.4 Security incident response
5.5 Learning from experience
Improved understanding of risk

Figure 2 Security life cycle

5.1 Overview

The security life cycle includes strategy and planning, prevention and detection, incident management and reviews from lessons learned. See Figure 2.

Holistic management of security helps prevent security incidents and makes it easier to respond and learn lessons about how to improve. The management of security should bring together consideration of physical security (see 6.1), personnel security (see 6.2), cyber security (see 6.3), technical security (see 6.4) and industry security (see 6.5).

5.2 Security strategy and planning

5.2.1 Overview

Organisations should align their security strategies with the Cross-Government Security Function Strategy. They should seek to protect government operations to the appropriate level, while enabling the functioning of government's services and operations.

Security plans should take into account incidents that have been reviewed and incident response plans. Security planning should be holistic, encompassing all aspects of good protective security.

5.2.2 Security response plans

Each organisation shall produce, and regularly test, a security incident management plan, describing how security incidents should be managed and resolved. This framework should be communicated to appropriate stakeholders. The incident management plan should include:

- activities as described in this functional standard and in the incident management technical standard
- the roles and responsibilities of individual officers
- measures for communication with personnel and the emergency services, especially at the time of the incident and period immediately following an incident
- a provision for a review of best practice

Security response plans shall be supported by policies, processes and systems to ensure reports and actions are received and can be acted on without undue delay.

Government organisations shall have management structures that ensure shared communications between human resources and security teams. The structures shall provide policies and procedures for detecting, reporting, responding to and handling incidents, including disciplinary measures, which are communicated to, and understood by, staff.

5.3 Prevention and detection

5.3.1 Security arrangements

Organisations should undertake a regular holistic assessment of the security arrangements that they have in place and assess whether these remain appropriate to the organisation's specific requirement. Day-to-day security activity in an organisation should be carried out in a way that avoids security incidents arising in the first place.

Security concerns, noted by anyone working for, or with, government including third party contractors, should be reported in a timely manner through clearly defined routes.

5.4 Security Incident Response

5.4.1 Incident reporting

A security incident, when detected, should be reported as soon as possible within the organisation's defined timeframe, so it can be investigated.

Those with security-related responsibilities shall understand their legal obligations for reporting incidents to their management boards and other interested parties, such as the Information Commissioner's Officer and Government Security Group.

Note: consider legislation including the General Data Protection Regulation (GDPR).

5.4.2 Incident response

The incident manager should handle the response to security incidents in accordance with the organisation's security response plans (see 5.2.2), including taking action on failures of personnel to comply with security policies and procedures. Lessons learned and updating of procedures shall be recorded (see 5.5).

5.4.3 Post response review

Following events, incidents or crisis situations, the organisation's response should be reviewed and the security response plan updated to include learning that can streamline the response process and to ensure that the same situation cannot be repeated. Identified vulnerabilities should be remediated and degree of risk should be reassessed. Organisations should implement necessary changes to their security governance and management framework or training that would prevent further occurrences.

5.5 Learning from experience

Learning from experience avoids repeating the same mistakes and helps spread improved practices to benefit current and future security arrangements.

Lessons should be continually captured from all levels of the organisation, holistically evaluated, and action taken to mitigate risk and facilitate continual improvement of security practices at cross-government and organisational levels.

6 Security practices

6.1 Physical security

The purpose of physical security measures is to ensure a safe and secure working environment for staff and visitors, protecting them against a wide range of threats (including theft, terrorism and espionage). Organisations should implement layered security measures in any government property or government supplier property that has government classified information, assets or people. These measures should complement each other, provide a proportionate degree of protection against diverse threats, and offer a contingency in the event of one measure failing.

Physical security measures should consider, but not necessarily be limited to:

- integrating physical security into designs of buildings to protect assets and enable modern ways of working
- designing a layout that mitigates the risks of having vulnerable space at the base of the building
- implementing protective and preventative measures to reduce the likelihood of damage and injury being caused to assets, whilst ensuring adherence to UK building regulations

Government organisations shall have:

- processes and plans in place to determine the appropriate physical security requirements through risk assessment
- mechanisms to implement internal and external security controls in a layered fashion that deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attack
- measures for controlling access and proximity to the most high-risk sites and Critical National Infrastructure assets

Consideration should be given to the physical environment in which civil servants, crown servants, military personnel and contractors operate. Consideration should be given to specific security control rooms and guard force areas. To ensure the effective running of government business, security of storage facilities shall be considered and appropriate controls around mail or deliveries applied. To manage risks to an organisation, measures to protect people and assets from an intruder should be in place as well as vehicle management to protect against vehicles being used as a weapon.

Government contractors processing or storing classified material on their own premises at SECRET or above shall be considered for Facility Security Clearance (List X) accreditation.

Buildings, systems and processes should be designed to incorporate features that are designed to avoid or prevent security incidents. GovS 004, Property shall be followed.

Note: See Annex C for a description of physical security standards.

6.2 Personnel security

The purpose of personnel security is to assure the government that the people it employs are suitable for work in sensitive roles. It also safeguards employees from exploitation as a result of their personal circumstances.

Government organisations shall deliver the appropriate combination of recruitment checks, security vetting and on-going personnel security aftercare to reduce the risk from insider threat [1].

Government organisations shall have consistent HR and personnel security policies and processes, including recruitment checks in accordance with national security vetting: clearance levels [7]. Prospective employees shall be subject to pre-employment screening checks and, where necessary, vetting. New staff, or those new to a role, should undergo a risk-based assessment for their suitability. Security clearances should be maintained and verified on an on-going basis and, where necessary, withdrawn. Processes shall be in place to ensure staff are aware of their obligations under the Civil Service Code and their responsibility to the Official Secrets Act (1989), and that breaches can result in disciplinary action.

Processes should be put in place to define:

- the basis for risk-based decisions to allow employees to undergo the national security vetting in parallel to check against the baseline personnel security standard
- the rationale for the relevant level of security clearance for different roles
- how vetting assessment, recommendations and decisions should be recorded and reported
- the approach to maintaining clearances, including the Annual Security Appraisal Form for Developed Vetting cleared personnel
- the process by which clearance levels are reviewed, and particularly when staff move into new roles
- the approach to handling refusal or withdrawal of clearances for both candidates at the recruitment stage and those already in employment
- the process by which security clearances are transferred to another government organisation, when an employee moves

Consideration should be given to the risk assessment of all individuals working on government business to limit the threats posed from insiders. This is likely to include risk assessment of roles, security considerations during recruitment, security assurance of individuals throughout their time within the organisation and alignment of organisational policies with security to outline expectations of staff in matters such as, though not limited to, travel overseas, use of information technology or use of social media. Exit procedures should also be in place to limit the risk of staff damaging the organisation upon exit.

Government contractors with employees that hold security clearances to SECRET or above should be considered for Industry Personnel Security Assurance accreditation [8]. GovS 003, Human Resources shall be followed.

Note: See Annex C for a description of personnel security standards.

6.3 Cyber security

The purpose of cyber security is to ensure the security of data and information. To operate effectively, the UK government needs to maintain the confidentiality, integrity and availability of its information, systems and infrastructure, and the services it provides. Organisations that handle government data and information shall meet the standards prescribed by HM Government [2].

All organisations using this standard shall have:

- an understanding, by all staff, of the expectations the organisation makes of them for the proper protection of information (including partner information) and understand where to seek help if they are unsure
- processes in place to identify and protect core assets and systems delivering essential functions

Organisations should take steps to detect cyber attacks and have a defined, planned and tested response to such incidents, especially when they impact sensitive information or key operational services.

Systems that handle sensitive information or deliver key operational services shall be protected from exploitation of vulnerabilities. Highly privileged accounts should not be vulnerable to cyber-attacks.

There should be a statement of assurance for all projects that shows evidence of assessing information and cyber risks, and the controls put in place. Organisational boards assessing risk should have the information to be able to identify major projects that have high information and cyber security risks. The organisation should have clear information and cyber security guidance and standards available to new projects. Organisations should have managed, risk informed, security controls to mitigate applicable risks while deterring, detecting and protecting against malicious or negligent behaviour.

Due consideration should be given to the protection of enterprise technology within an organisation and ensuring that infrastructure is not vulnerable to common cyber-attack. Cyber security also comprises the protection of end-user devices and email used throughout the organisation. Due consideration should also be applied to the protection of digital services operated by an organisation and cyber threats such as, though not limited to, identity theft, breaches of access and intellectual property theft.

Note: See Annex C for a description of cyber security standards.

6.4 Technical security

The purpose of technical security measures is to holistically protect sensitive information and technology from close access acquisition or exploitation by hostile actors, as well as any other form of technical manipulation. Technical security also relates to the protection of security systems from compromise and/or external interference. Government organisations shall have:

- policies and processes to control the use of mobile devices in sensitive areas
- staff awareness about the risks of using personal devices in government buildings
- security management processes that facilitate staff to conduct sensitive conversations and meetings in an appropriate environment
- processes to maintain the technical integrity of the government estate, including the potential compromise of electromagnetic and other emanations
- security managed estate improvement plans to mitigate the compromise of the building structure from close access or standoff attack

Note: See Annex C for a description of technical security standards.

6.5 Industry security

The purpose of managing industry security is to protect the government from threats relating to contractors and suppliers having access to classified information, assets and estates, all of which are vulnerable to compromise by adversaries.

The aims and intent of this standard are applicable to government contractors that access (or protect) classified information and assets, or employ staff with National Security Vetting clearances. The applicability and specific mandatory requirements for government contractors are identified in supplementary documents including: Security Requirements for Facility Security Clearance (List X) Contractors, Industrial Security Departmental Responsibilities, Contractual Process and the Industry Personnel Security Assurance policy.

Security threats to the government that seek to exploit vulnerabilities in industry security should be identified and risks assessed throughout the life-cycle of a contract, beginning before contracts are let. Appropriate security clauses should be added to contracts. To facilitate this, organisations shall:

- develop a culture whereby individuals understand that mitigating threats in industry is a collective responsibility whilst contract managers are responsible for the security of their assigned suppliers
- take a holistic approach to supplier assurance that considers and mitigates the risks posed to physical, personnel and cyber security
- set and communicate minimum contractual security requirements to suppliers.
- conduct frequent assurance to verify that security measures are being met and remain adequate
- build security considerations into departmental contracting processes, including the requirement for suppliers to notify contract managers of security incidents or changes to the security profile of their organisation
- ensure procurement is at the most suitable classification and suppliers abide by Facility Security Clearance Assurance (List X) and Industry Personnel Security Assurance policies if applicable

Organisations should meet the relevant commercial and industrial security policies prescribed by HM Government [5]. See also GovS 008, Commercial.

Note: See Annex C for a description of industry security standards.

6.6 Security risk management

6.6.1 Defining and establishing risk management procedures

The purpose of security risk management is to understand security risks, which helps government organisations reduce the opportunities for threat actors to cause harm to government assets.

Government organisations shall establish policies, processes and capabilities to enable understanding of the risks to the organisation and its assets - including its people, information, the services it provides and the customers of those services. That understanding should be achieved through risk assessment, relevant to each organisation's own context, by skilled people using appropriate mechanisms, and by the establishment of risk appetites.

Responsibilities for risk management and associated decision-making shall be defined, with the Accounting Officer holding overall accountability and ensuring that practical direction is set on what aspects of the organisation and its activities and services are to be protected, and articulating risk appetites in terms of the level of acceptance of risk in respect of those aspects. The Accounting Officer may delegate responsibility to make decisions on the identification and management of risks, with identified risk owners.

6.6.2 Organisational risk management

Organisations shall have policies and processes in place to conduct regular risk and vulnerability assessments for their organisations and their assets. Preventative measures should also be developed to:

- mitigate the risk of a security incident occurring
- prevent further occurrences
- reduce the impact of incidents

This includes reviewing resilience planning for critical assets, in particular, those identified as critical national infrastructure (see 6.8).

Security processes should be designed and operated to mitigate the identified risks within agreed tolerances, and to keep pace with security risks as the threat and vulnerability landscape changes. Planning and testing processes and controls should be designed and operated to identify and inform risks and risk management.

Organisations shall be familiar with how the National Technical Authorities (the National Cyber Security Centre, Centre for the Protection of National Infrastructure [6], and UK National Authority on Counter-Eavesdropping) can help identify and manage risk. Similarly, they should be familiar with the assistance the Government Security Centres can provide. They should work with the Government Security Profession to identify, source and support the skilled resources needed.

Organisations should establish a system for identifying security risks in a register, and for exposing these risks to the appropriate governance boards for review at appropriate intervals.

6.6.3 Business continuity

Security objectives should be taken into account in an organisation's business continuity plans and processes, so that a security failure or compromise does not lead to unwarranted loss of operations or service.

6.7 Information management

The purpose of information management is to implement protective security measures that mitigate insider threat across government and ensure consistency and efficiency between government organisations.

Access to classified, sensitive or critical information and key operational services should only be provided to identified, authenticated and authorised users or systems, and proportionate risk mitigation controls should be applied.

Information assets shall be classified according to HM Government classification policy.

All organisations using this standard shall have:

- an understanding of their policies and processes to protect sensitive data holdings
- policies, systems and processes for information handling that are compliant with HM Government information security policies and standards and relevant legislation and regulations, such as the Data Protection Act 2018 and the Public Records Act 1967
- regular training and education for all staff, and contractors who handle government information, on appropriate information security measures, including refresher training. Through proper education and awareness provisions, organisations should ensure that users are able to understand and comply with both their department's local policies and wider government policies

These information security policies should be kept up to date and should cover:

- the classification of information
- processes for the appropriate handling, storage, sharing, and destruction of information based on its marking
- systems and processes for protecting information when working remotely
- roles and responsibilities in the information handling chain
- if an organisation shares information with international partners, it shall have policies and processes in place to securely manage international classified exchanges that are compliant with government policies and standards

6.8 Critical assets and services

The purpose of critical assets and services is for organisations to identify and catalogue the critical assets (including information) they hold and key operational services they provide, so that they are aware of their existence and can take the necessary mitigating action. This includes understanding the technologies used, other dependent services (such as power, cooling, data), the supply chain implications and the impact of loss of services.

6.9 Capability, capacity and resources

The purpose of capability, capacity and resource management is to balance the supply and demand for appropriate resources (such as people, equipment, material and facilities) that can be deployed when needed. Resources might be sourced from within the government, through recruitment or from the supply chain. GovS 003, Human Resources and GovS 008, Commercial shall be followed.

A comprehensive view of future resource needs to address security vulnerabilities and responses should be developed and maintained, with possible shortfalls identified and addressed. Resources should be secured or developed to meet the planned needs. If insufficient resources are available, work should be re-planned to reflect such constraints.

Organisations should call upon the advice available to them across each area of government security through the Government Security Centres.

6.10 Security culture, education and awareness

The purpose of security culture, education and awareness is to enable the government to function effectively. This will be done through a security culture of unambiguous personal accountability and an understanding of managing risk, responsibility and reputation.

Organisations using this standard shall have:

- a security culture publicised and led by example from the top of organisations, with the Accounting Officer (or equivalent in an arm's length body) and executive board following the relevant processes and policies
- an open dialogue on security, including encouraging the reporting of near misses to facilitate lessons learned

Security education and awareness activities are intended to ensure that members of the workforce are aware of and understand the organisation's security policies, processes, systems and controls. This will help to mitigate the risk of staff being responsible for data breaches and other security incidents and ensure that business objectives are delivered safely and securely. Security education and awareness activity should include a combination of:

- induction material and programmes for employees and contractors
- periodic education and awareness events and campaigns for employees and, where appropriate, contractors on matters of importance to the secure delivery of business objectives
- continuously available Security Education and Awareness products to support locally led initiatives
- specific training and briefings for particular audiences

Organisations shall ensure that new joiners have immediate access to induction material and core learning on security responsibilities and obligations. Induction should include, but not be limited to:

- the necessary policies and processes to be followed; the availability of facilities and tools appropriate to the role being undertaken
- a formal briefing on why and how security is important to the organisation and the particular role concerned
- early and on-going training required
- the granting and review of appropriate access to information and other systems in accordance with the role undertaken and the level of security clearance granted

Organisations shall have in place an ongoing and regularly reviewed and updated programme of Security Education and Awareness activities, tied to the attainment of business objectives and in line with security policies. The programme should include: appropriate threat briefings, other communications and learning materials for senior officials, line managers and other generic audiences, as well as specific briefings and learning materials for more specialist audiences with particular exposures, needs and security obligations.

Education and awareness activities should highlight personal accountability and encourage appropriate security behaviours, with incentives to deliver this tied to the organisation's HR policies and procedures. Communications and monitoring shall be in place to ensure all staff undertake mandatory training courses, briefings or e-learning. These should be supported by management intervention, reporting and assurance.

GovS 003, Human Resources shall be followed, in support of this area of activity, guided by the security profession.

A. References

All references are correct at the time of publication, users should check for updated versions.

ID	Description
	Government references
1	Government Security Group, *Government baseline personnel security standard* (2018)
2	Government Security Group, *Minimum Cyber Security Standard* (2018)
3	HM Treasury, *Orange Book: Management of risk – Principles and Concepts* (2020)
4	Government Security Group, *Government security roles and responsibilities* (2018)
5	Government Security Group, *Industrial Security Policies* (collection)
6	National Cyber Security Centre, *Advice and guidance*
7	Ministry of Defence and United Kingdom Security Vetting, *National security vetting: clearance levels* (2020)
8	Government Security Group, *HM Government Security Classifications Policy* (2018)

B. Glossary

See also the **common glossary of definitions** which includes a list of defined terms and phrases used across the suite of government functional standards. The glossary includes the term, definition, and which function owns the term and definition.

Term	Definition
assurance	A general term for the confidence that can be derived from objective information over the successful conduct of activities, the efficient and effective design and operation of internal control, compliance with internal and external requirements, and the production of insightful and credible information to support decision making. Confidence diminishes when there are uncertainties around the integrity of information or of underlying processes.
compromise	In the context of security, compromise is bringing an asset (including people, property or information) into disrepute or danger.
crisis (security)	In the context of security, a crisis is a direct threat or act against staff or assets that can or has caused a loss of life or critical business function.
critical national infrastructure	Those facilities, systems, sites, information, people, networks and processes necessary for a country to function and upon which daily life depends.
cyber security	Protective cyber security measures put in place to mitigate against the consequences of an external cyber attack on government information, personnel or infrastructures.
defined (way of working)	In the context of standards, defined denotes a documented way of working, which people are expected to use. This can apply to any aspect of a governance or management framework, for example processes, codes of practice, methods, templates, tools and guides.
developed vetting	A level of security clearance which allows unsupervised access of material up to and including “TOP SECRET” on a regular basis.
established (way of working)	In the context of standards, ‘established’ denotes a way of working that is implemented and used throughout the organisation. This can apply to any aspect of a governance or management framework, for example processes, codes of practice, methods, templates, tools and guides.
event (security)	In the context of security, an event is a disruptive but non-threatening organised event in your department or building, or an event in the public space, which requires security planning and mitigations to be put in place.
governance	Governance defines relationships and the distribution of rights and responsibilities among those who work with and in the organisation. It determines the rules and procedures through which the organisational objectives are set, and provides the means of attaining those objectives and monitoring performance. Importantly, it defines where accountability lies throughout the organisation.

Term	Definition
governance and management framework	A governance and management framework sets out the authority limits, decision making roles and rules, degrees of autonomy, assurance needs, reporting structure, accountabilities and roles, and the appropriate management practices and associated documentation needed to meet this standard.
incident (security)	In the content of security, an incident is any circumstance that arises where assets may be damaged, compromised, lost or leaked as a result of failure of policy or codes of conduct, existing security measures or controls, or something that requires an action/response following a direct threat or individual action, or to prevent one of the above. These could be accidental or deliberate acts by those internal or external to the department.
insider threat	The threat posed by staff, contractors or contracted third parties not following or deliberately disregarding established policies.
organisation	An organisation, in the context of government functional standards, is the generic term used to describe a government department, arm's length body, or any other entity that is identified as being within scope of a functional standard.
personnel security	The practice of ensuring the security of government information and infrastructure against threats arising from government personnel.
physical security	The practice of protecting elements of government infrastructure, estates and personnel against attacks or compromises in the physical (i.e. tangible, real-world) environment.
plan	A plan sets out how objectives, outcomes and outputs are to be delivered within defined constraints, in accordance with the strategy.
prevention (security)	In the context of security, prevention is the action of stopping a security incident arising.
property	Land, buildings, infrastructure or facilities held in any form of tenure.
protective security	The term used to define physical, personnel, cyber, technical and industry security working in concert to protect an organisation and its assets.
risk appetite	The amount of risk the organisation, or subset of it, is willing to accept.
risk tolerance	The threshold levels of risk exposure that, with appropriate approvals, can be exceeded, but which when exceeded will trigger some form of response (for example, reporting the situation to senior management for action).
security breach	The confirmed compromise of government assets without permission or authority. This includes people, property or information.
security threat	A possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.

Term	Definition
security vulnerability	A weakness that could be exploited by an adversary.
service catalogue	A list of operational security services that Government Security Centres provide to their organisations.
strategy	An outline of longer term objectives, outcomes and outputs, and the means to achieve them, to inform future decisions and planning.

C Subject specific security standards

At the time of going to print, this functional standard is underpinned by six subject specific standards, which define the requirement for physical, personnel, cyber, technical, industry and incident management. As far as possible the security standards define outcomes, allowing organisations flexibility in how the standards are implemented, dependent on their local context. The definition of 'important' and 'appropriate' are deliberately left open, so that organisations can apply their own values based on their particular circumstances. An organisation's leaders are accountable for the effectiveness of these decisions.

Subject specific standard: Physical

This document provides a specification for the layered security measures expected to be delivered as standard at a government occupied building. Consideration should be given to the physical environment in which civil servants, government departments, all crown servants, and HM Government contractors operate. This is likely to include those areas on the front line, including the reception or receiving areas of any government building that protect publicly available spaces. It also encompasses staff working areas in OFFICIAL and above working spaces. Consideration should be given to specific security control rooms and guard force areas. To ensure the effective running of government business, security of storage facilities must be considered and appropriate controls around mail or deliveries applied. To manage risks to an organisation, measures to protect people and assets from an intruder should be in place as well as vehicle management to protect against vehicles being used as a weapon.

Subject specific standard: Personnel

This document provides organisations with details of the minimum personnel security standards which, when met, will mitigate against the insider threat across government, and ensure consistency and efficiency among organisations.

Consideration should be given to the risk assessment of all individuals working on government business to limit the threats posed from insiders. This is likely to include risk assessment of roles, security considerations during recruitment, security assurance of individuals throughout their time within the organisation, and alignment of organisational policies with security to outline expectations of staff in matters such as, though not limited to, travel overseas, use of information technology or use of social media. Exit procedures should also be in place to limit the risk of staff damaging the organisation upon exit.

Subject specific standard: Cyber security

This document defines the minimum security measures that organisations are required to implement with regards to protecting their technology and digital services to meet their security obligations. Compliance with this standard can be achieved in many ways, depending on the technology choices and business requirements in question. For digital services, this set of standards is complementary to the Digital Service Manual. Consideration should be given to the protection of enterprise technology within an organisation and ensuring that any infrastructure is not vulnerable to common cyber attack. Cyber security also comprises the protection of end user devices and email used throughout the organisation. Consideration should also be given to the protection of digital services operated by an organisation and cyber threats such as, though not limited to, identity theft, breaches of access and intellectual property theft.

Subject specific standard: Technical security

This document specifies the baseline requirements organisations must meet to mitigate against the threat of technical attack or accidental exposure of information. Compliance may be achieved in a variety of ways and consideration should be given to the organisational specific business context, location and techno-physical environment.

Consideration should be given to the range of targets susceptible to technical attack including, but not limited to, tangible physical and digital assets, as well as intangible assets such as sensitive conversations and phone calls, and electromagnetic emanations.

To manage the risks associated with technical security the range of approaches, including distanced standoff as well as both quick and deep plant close access, should be considered.

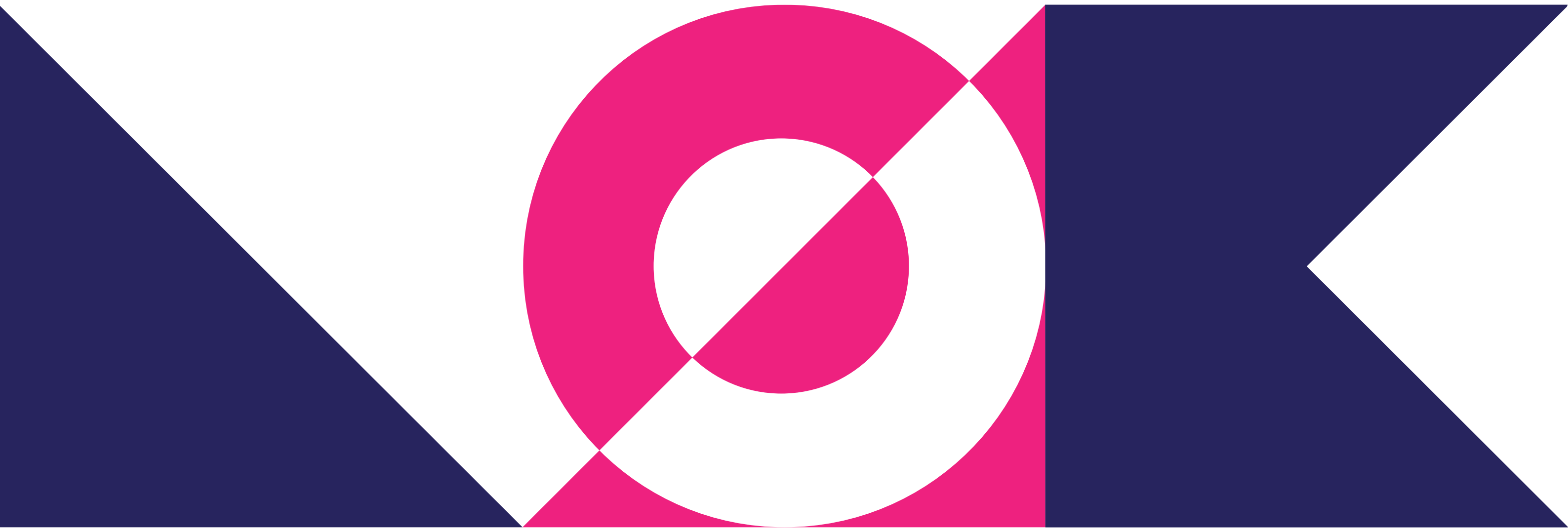
Technical security involves the lifecycle of an asset and should be considered through construction or purchase, use, and demolition or disposal. Use of both ongoing and targeted inspections by approved technical security professionals, security by design and active countermeasures is to be considered as a part of meeting technical security requirements.

Subject specific standard: Industry security

There are a number of supplemental documents relating to the security arrangements between contracting authorities and HM Government suppliers. Facility Security Clearance (List X) and Industry Personnel Security Assurance policies cater for the physical and personnel aspects of contracting at SECRET or above. These are joined by more general guidance on departmental responsibilities as well as policy on security in the contractual process. Separately, there is a Government Supplier Assurance Framework to provide departments with the tools and principles to manage supplier risk.

Subject specific standard: Incident management

This document defines the minimum measures that organisations are required to implement with regards to managing security events, incidents and crises. In all cases relevant guidance should be followed.



DocuSign Envelope ID: 7B9F5B3F-230B-4AE9-BAE5-70B9110378D5

	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]			
[redacted]																							
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]		[redacted]		[redacted]	[redacted]							[redacted]					[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]							[redacted]	[redacted]				[redacted]
[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]																[redacted]
[redacted]	[redacted]			[redacted]		[redacted]																	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]		[redacted]	[redacted]							[redacted]	[redacted]				[redacted]
[redacted]																							
[redacted]										[redacted]										[redacted]			[redacted]
[redacted]					[redacted]					[redacted]													[redacted]
[redacted]										[redacted]										[redacted]			[redacted]
[redacted]										[redacted]										[redacted]			[redacted]
[redacted]										[redacted]													[redacted]
[redacted]																							
[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]																	[redacted]
[redacted]																							
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]			[redacted]								[redacted]								[redacted]
[redacted]			[redacted]	[redacted]			[redacted]																[redacted]
[redacted]			[redacted]				[redacted]																[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]			[redacted]																[redacted]
[redacted]																							
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]							[redacted]												[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]													[redacted]						[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]									[redacted]
[redacted]																							
[redacted]					[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]			[redacted]
[redacted]																							
[redacted]																						[redacted]	[redacted]
[redacted]																						[redacted]	[redacted]
[redacted]																						[redacted]	[redacted]
[redacted]																						[redacted]	[redacted]
[redacted]																						[redacted]	[redacted]
[redacted]																							
[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]																	[redacted]
[redacted]																							
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]						[redacted]	[redacted]	[redacted]				[redacted]
[redacted]			[redacted]	[redacted]	[redacted]	[redacted]	[redacted]																[redacted]
[redacted]																							
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]												[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]											[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]												[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]												[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]					[redacted]		[redacted]											[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]																[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]					[redacted]		[redacted]						[redacted]						[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]				[redacted]
[redacted]	[redacted]			[redacted]		[redacted]											[redacted]						[redacted]
[redacted]																							
[redacted]										[redacted]										[redacted]			[redacted]
[redacted]																							
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]																	[redacted]
[redacted]																							
[redacted]		[redacted]	[redacted]	[redacted]			[redacted]																[redacted]
[redacted]				[redacted]			[redacted]								[redacted]	[redacted]							[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]			[redacted]																[redacted]
[redacted]																							
[redacted]	[redacted]			[redacted]					[redacted]		[redacted]							[redacted]					[redacted]
[redacted]		[redacted]						[redacted]	[redacted]		[redacted]										[redacted]		[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]		[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]				[redacted]		[redacted]					[redacted]												[redacted]
[redacted]	[redacted]			[redacted]		[redacted]											[redacted]						[redacted]
[redacted]																							
[redacted]	[redacted]		[redacted]	[redacted]		[redacted]																	[redacted]
[redacted]																							
[redacted]			[redacted]	[redacted]			[redacted]																[redacted]
[redacted]																							
[redacted]			[redacted]	[redacted]			[redacted]	[redacted]			[redacted]												[redacted]
[redacted]		[redacted]		[redacted]				[redacted]			[redacted]												[redacted]
[redacted]	[redacted]			[redacted]		[redacted]											[redacted]						[redacted]
[redacted]																							
[redacted]	[redacted]		[redacted]	[redacted]		[redacted]																	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]																			[redacted]