Technology Notices Accreditation Feasibility Study

Final Report

August 2025

PUBLIC

Ofcom

Table of Contents

1. Executive Summary

Under section 121 of the Online Safety Act 2023, Ofcom has the power to issue a notice to the provider of a particular regulated user-to-user or regulated search service ('Part 3 service'), where considered necessary and proportionate to deal with terrorism or child sexual exploitation and abuse ('CSEA') content (or both). This notice could require a provider to use technology that has been accredited, by Ofcom or a third party appointed by Ofcom, against 'minimum standards of accuracy' ('accredited technology'). **To enable this power and be able to issue Technology Notices, Ofcom needs to establish an accreditation scheme** for specific technologies that may be used to identify terrorism and/or CSEA content once the Secretary of State for Science, Innovation and Technology ('Secretary of State') approves and publishes the minimum standards of accuracy.

From April 2025 to August 2025, PUBLIC was commissioned by Ofcom to undertake an independent feasibility study of the accreditation scheme related to Ofcom's Technology Notice power. This research developed a **process map for establishing, operating and maintaining the technology accreditation scheme**, assessed the operations, costs, timing and resources requirements, and identified relevant constraints, risks and potential mitigations for the scheme.

This report contains findings based on evidence gathered from:

- **24 interviews** with His Majesty's Government ('HMG') departments, other regulators, online safety technology providers, civil society organisations, and accreditation scheme operators for other technologies;
- **7 survey responses** on the costs and resourcing requirements involved in setting up and operating similar technical infrastructure and accreditation schemes;
- **A desk-based review** of relevant Ofcom publications and consultation materials, analyses of comparable accreditation frameworks, government guidance on handling sensitive data and technology infrastructure, and historical public sector procurement data from similar initiatives.

This research found that:

- An effective accreditation scheme should be **transparent, independent, and accessible**. Applicants would benefit from clear guidance, structured opportunities for feedback, and a streamlined process that minimises administrative burden. Potential applicants emphasised that their willingness to participate depends on whether the scheme yields tangible commercial benefits, such as enhanced credibility, improved market access, and procurement advantages, and whether the time, cost, and effort required are worthwhile.
- Ahead of launch, Ofcom needs to define the scheme's **governance and delivery model**, including the degree to which responsibilities are retained in-house or delegated to third parties. These responsibilities include

scheme design and approval, assessor appointment and training, and delivery of assessments. Governance and delivery models range from a minimal oversight model, in which delivery is largely outsourced, to a fully in-house model in which Ofcom retains end-to-end control. These choices affect Ofcom's operational oversight, exposure to delivery risks, and internal resourcing requirements.

- The recommended approach is to adopt a **phased, modular rollout**: starting with a lean delivery model in Year 0 to enable rapid implementation with reduced complexity, followed by a transition to a more formalised structure as the scheme stabilises.
- A strategic decision for Ofcom is **whether to include Independent Performance Testing ('IPT')**, which represents the most technically complex and cost-intensive element of the scheme. Delivering IPT requires secure handling of relevant testing datasets and the establishment of secure testing infrastructure.
- **Key technical considerations for IPT** include the hosting model (e.g., on-premise or cloud-based), the procurement and ownership of testing datasets, and the architecture of the testing environment (e.g., Application Programming Interface ('API') access or managed testing environments). Crucially, Ofcom will need to determine how to lawfully acquire and manage content for testing categories. Procuring illegal content in particular will necessitate formal partnerships and legal agreements supported by strong governance and compliance frameworks.
- Our research estimates that the scheme, **including the IPT**, would require an initial one-off investment in the range of £1.2 million to £9.3 million in Year 0, with recurring annual costs during accreditation periods of £340,000 to £1.1 million thereafter, depending on delivery options and technical complexity. **With the Audit Based Assessment ('ABA') only**, the estimated cost would be £233,000 to £1.8 million in Year 0, with recurring annual costs of £146,000 to £628,000. Initial design and establishment are expected to take between 6 and 14 months. Once operational, delivery timelines may vary based on assessment depth and scheme formality, with end-to-end accreditation potentially ranging from 4 to 9 months.
- **The principal cost drivers** fall into three categories:
    - **Operations:** Costs include assessor time, internal staffing to support accreditation processes, administrative support, and training.
    - **Technical Infrastructure:** Especially relevant for IPT, this includes secure hosting, computing capacity, cybersecurity measures, and ongoing system maintenance. Establishing a secure environment for testing will require significant capital and operational expenditure.
    - **Data:** IPT delivery will require access to both benign and illegal content datasets. This involves costs for licensing, storage, secure access, and compliance.

- **Projected demand** is estimated at approximately 40 to 80 applicants per period. Demand levels have limited impact on overall costs, aside from staffing, where costs scale with application volumes. Most other expenditures are expected to remain stable.
- As Ofcom prepares to establish the accreditation scheme, it must address a series of critical decisions spanning strategic, technical, and architectural dimensions. The following section outlines these key decision points and associated considerations in detail.

DISCLAIMER: This report provides PUBLIC's views and findings from evidence gathered from desk research, interviews and surveys. It does not set out Ofcom's views in this area or necessarily represent any policy position that Ofcom may adopt as the online safety regulator. Furthermore, while a significant cross-section of relevant stakeholders were engaged for this report, it may not capture the perspectives of all stakeholders.

2. Key Decisions for Ofcom

Implementing the accreditation scheme will require Ofcom to make a series of strategic and operational decisions that **shape how the scheme moves from design to delivery**. These decisions will define the scheme's structure, scope, and long-term sustainability, directly influencing its credibility, efficiency, and ability to adapt to evolving risks and technologies. They will also determine key cost, resourcing, and timing requirements.

This section outlines the **core decision areas** Ofcom will need to address to set up and operationalise the scheme effectively, grouped under two categories: (1) scheme design and (2) technology and architecture.

2.1 Scheme Design Decisions

Following approval and publication by the Secretary of State ('SoS') of relevant minimum standards of accuracy, Ofcom will need to determine the core features of the accreditation scheme, including its overall structure, scope, and how providers engage with each stage of the process. These design choices will shape the scheme's legal complexity, operational demands, and its ability to adapt to evolving technologies.

- **What level of testing will be included in the accreditation scheme?** Ofcom's Technology Notice consultation included two elements: an Audit-based Assessment ('ABA') and Independent Performance Testing ('IPT'). The decision about whether the scheme will incorporate one or both of these has significant implications across several dimensions. From a legal perspective, incorporating IPT introduces additional risks and compliance requirements, particularly in relation to access and handling of CSEA, which may restrict who can participate in delivery. In terms of technical infrastructure, IPT would require a secure testing environment, high-performance computing resources, and controlled access to sensitive datasets. Cost-wise, these additional requirements would increase upfront and ongoing expenditure, including infrastructure, staffing, and dataset licensing or development. Finally, including IPT could enhance the robustness of the scheme by providing independent validation of real-world performance, though it may also increase entry barriers for applicants and discourage participation.

- **What delivery model will be used: in-house, outsourced, or hybrid?** The delivery model will determine Ofcom's level of direct operational involvement. In-house delivery offers greater control but demands more internal resources and infrastructure. Outsourcing can reduce internal workload but raises challenges around oversight, quality assurance, and data protection. Assuming that suitable outsourcing partners could be found, it would also require the establishment of formal legal agreements

and contracts. A hybrid model may strike a balance, allowing Ofcom to retain control over sensitive functions while leveraging external capacity where appropriate.

- **If outsourced, would Ofcom appoint multiple providers or seek to consolidate functions where feasible?**
  Assuming that suitable outsourcing partners could be found, Ofcom would need to consider whether to appoint separate providers for different stages of the process (e.g. application screening, ABA, and IPT), or to consolidate delivery under a smaller number of partners. This decision will affect contract complexity, accountability mechanisms, and whether there are enough capable providers to deliver each part of the scheme to the required standard.

- **Is age assurance in scope (e.g., use of age estimation to identify children in sexual content)?**
  Some age assurance tools use biometric analysis to estimate the age of individuals depicted in sexual content, potentially to assess whether material constitutes CSEA. Ofcom must determine whether it would accept applications for such technologies to be accredited under the scheme. This edge case affects the eligibility of certain age assurance providers and could expand the scheme's coverage.

- **Will there be an appeal process, and at what stage(s)?**
  Ofcom needs to decide whether applicants are allowed to challenge accreditation outcomes, and at which stages of the process (e.g. following ABA, IPT, or final decisions). A structured appeals process would enhance procedural fairness and transparency, and could draw on best practices from other schemes such as Age Check Certification Scheme ('ACCS') and Cyber Essentials.

- **How long will accreditation remain valid?**
  The validity period will affect administrative workload, provider certainty, and the scheme's ability to keep pace with technological change. Although a four-year cycle has been proposed, Ofcom will need to assess whether this duration is appropriate given the rate of tool development and the potential for reduced performance over time.

- **Will re-accreditation be required only after a fixed period, or also triggered by events such as model updates?**
  In addition to periodic re-accreditation, Ofcom may consider introducing event-based triggers, such as significant version updates. One potential approach is to link accreditation to a specific version of a technology. Under this approach, significantly updated versions would require re-accreditation before they could be required in a Technology Notice, while

the originally accredited version would remain valid until the end of the fixed accreditation period. Further work may be required to determine what constitutes a 'significant' update in this context.

2.2 Technology and Architecture Decisions

If Ofcom **includes IPT** within the scheme, a number of interrelated technology and architecture decisions will need to be resolved to ensure lawful, secure, and scalable testing.

- **How will datasets be sourced (benign, CSEA, terrorism)?**
  Ofcom needs to determine how to lawfully access and manage testing datasets. These datasets will be determined by the types of technologies that Ofcom chooses to accredit, however they will fall into the following broad categories

    - *Benign data*: Procure or compile diverse, representative datasets to support false-positive testing, including edge cases.
    - *Illegal data (CSEA and terrorism)*: Identify lawful access routes to these datasets, particularly CSEA content, which remains tightly regulated. While legal provisions now allow access in defined cases, the number of organisations eligible to handle this material remains limited. Access will continue to require careful governance, secure environments, and formal agreements with authorised data holders.

  Note also that data requirements may vary with respect to media types (i.e. images, video, Uniform Resource Locators ('URLs'), hashes, texts), demographic coverage, and sampling strategies must be defined to ensure fair and meaningful assessments across tool types (e.g., Artificial Intelligence ('AI') classifiers, hash matching).

- **Where will IPT be hosted, on-premises, cloud, or hybrid?**
  Ofcom needs to determine a hosting model that balances compliance, security, and cost.

  For CSEA content, cloud hosting is not legally prohibited but would require exceptionally high safeguards due to the material's criminal nature and sensitivity. These include strict access controls, full auditability, strong encryption, and clear retention and detention policies. In practice, stakeholders expressed a preference for on-premises environments, due to concerns around legal defensibility, operational control, and reputational risk. Some also recommend UK-only hosting to mitigate cross-border legal risks and support evidentiary integrity.

  For terrorism and benign content, cloud or hybrid models may offer greater flexibility, as these data types are generally subject to fewer legal

constraints. Ofcom may choose to host some datasets directly and tailor hosting configurations based on content type, sensitivity, and operational cost.

Different infrastructure models may be adopted for different content types to reflect varying legal and security requirements.

- **What testing deployment model will be used for IPT?**
  Ofcom needs to determine how submitted technologies will interact with test datasets during IPT. The chosen testing deployment model will affect the scheme's legal defensibility, operational complexity, and resource requirements. Each broad approach - ***outsourcing*** *(third-party testing),* ***endpoint access*** *(remote access by developers), or a* ***fully managed environment*** *(contained, in-house testing)* - involves distinct trade-offs between control, security, and delivery effort (see 'Phase 1: Establishment - Technical Infrastructure - Delivery Model Considerations; for a full explanation of each model and its implications). This decision is especially sensitive for CSEA content, where legal constraints significantly limit viable options. Terrorism and benign datasets may offer greater flexibility.

  A one-size-fits-all approach may not be suitable across all content types. While a fully managed environment could, in principle, be used for all datasets, this may introduce unnecessary cost and operational burden for some types of content. For CSEA data, a tightly controlled environment with stringent physical, digital, and procedural safeguards is likely required due to the material's criminal and sensitive nature, and the associated legal and safety obligations. In contrast, terrorism and benign datasets may allow for more flexible deployment models. Tailoring approaches by content type could improve suitability, scalability, and legal robustness. However, doing so would increase technical complexity, staffing demands, and the risk of fragmented delivery. Ofcom will need to weigh these trade-offs carefully when determining the most appropriate deployment strategy for IPT.

3. Introduction

3.1 Policy Context

Under the Online Safety Act, providers of Part 3 services have a range of new duties. They must assess, manage and mitigate the risks of harm from illegal content or activity on their platforms. They must also take or use proportionate measures to prevent users from encountering 'priority' illegal content by means of their regulated services. Ofcom has published its Illegal Harms Codes of Practice detailing recommended measures to fulfil these obligations and may enforce compliance where necessary.

Ofcom also has additional powers to specifically tackle two categories of priority illegal content: terrorism and CSEA content. Where it considers it necessary and proportionate, Ofcom may issue a Technology Notice requiring a Part 3 service provider to use an accredited technology to:

- Identify and/or prevent individuals from encountering terrorism content communicated publicly, and/or
- Identify and/or prevent individuals from encountering CSEA content communicated publicly or privately.

Alternatively, Ofcom may require a Part 3 service provider to use best endeavours to develop or source technology meeting the minimum standards of accuracy to deal with such CSEA content. However, this aspect of Ofcom's Technology Notice power is not the focus of this report.

Before a notice can be issued, the relevant technology must have been accredited against minimum standards of accuracy approved and published by the SoS. To enable this, Ofcom needs to establish and operationalise an effective technology accreditation scheme. In December 2024, Ofcom published a consultation,[1] setting out its policy proposals for advice to the SoS on how to set minimum standards of accuracy, which technologies would be accredited against. Ofcom's proposed approach is to assess the accuracy of technologies through an ABA process as a first step in all cases, with a proposed additional, supplementary stage of IPT for technologies that pass the initial ABA.

3.2 Project Objective

In April 2025, Ofcom commissioned the external consultancy, PUBLIC, to conduct a feasibility study on how to effectively establish and operationalise an accreditation process for technologies designed to detect terrorism and CSEA content. This report provides PUBLIC's views and findings from evidence gathered from desk research, interviews and surveys. It does not set out Ofcom's

[1] Ofcom, Technology Notices to deal with terrorism content and/or CSEA content. Consultation on policy proposals for minimum standards of accuracy for accredited technologies, and guidance to providers, 2024

views in this area or necessarily represent any policy position that Ofcom may adopt as the online safety regulator. Furthermore, while a significant cross-section of relevant stakeholders were engaged for this report, it may not capture the perspectives of all stakeholders.

This project provides a practical, evidence-based assessment of what would be required to design, establish, and operate a scheme to accredit technologies in line with proposals included in Ofcom's December 2025 consultation.[2] It examines the end-to-end accreditation process, covering both an ABA model and a combined model that incorporates supplementary IPT. It also explores potential delivery models, considering whether the scheme could be delivered by Ofcom, by a third party, or through a hybrid approach.

In addition, the study provides indicative estimates of the likely costs, staffing needs, and timeframes involved in setting up and running the scheme, depending on which models and steps are ultimately adopted. It also identifies key operational constraints and risks, along with potential mitigations to address them.

Overall, the aim is to provide Ofcom with a clear evidence base to inform its decision-making and recommendations to the SoS on minimum standards of accuracy and the subsequent design and delivery of the accreditation scheme, supporting the proportionate and effective use of its Technology Notice powers under the Online Safety Act. Ofcom will utilise this report, along with other relevant evidence (including responses to its recent consultation) to inform its advice to the SoS on minimum standards of accuracy and its approach to accreditation. However, it is ultimately for the SoS to approve and publish the final minimum standards of accuracy (not Ofcom), and it is possible that the minimum standards of accuracy published by the SoS are different to those recommended by Ofcom.

[2] Ofcom, Consultation: Technology Notices, December 2024

4. The Process Map

This section sets out how Ofcom could set up and run a technology accreditation scheme in practice. It provides a clear view of the key phases and activities involved, beginning with the scheme's establishment and continuing through its operation, from initial application to accreditation and ongoing monitoring. It also explores how delivery responsibilities could be shared between Ofcom and third-party organisations, and outlines potential governance arrangements to ensure effective oversight and management throughout the scheme's lifecycle. Finally, it provides detailed consideration of the steps required to make the scheme operational in practice.

4.1 Overview

This section provides a high-level summary of the accreditation process and the potential delivery models. It introduces the overall structure of the scheme, outlining the three core phases - **Establishment**, **Operationalisation and Maintenance** - and explains how the process moves from the scheme's initial setup through to application, assessment, and final accreditation.

Alongside the process design, this section sets out the delivery model options for the scheme, highlighting the potential roles of Ofcom and third-party organisations in delivering different elements of the process.

4.1.1 Accreditation Process at a Glance

The first phase of the process map focuses on the **establishment** of the accreditation scheme, setting out the key tasks required to design and implement the technology accreditation framework. For this phase, we use *'Tasks'* to describe actions which may happen in parallel.

The second phase of the process map focuses on the **operationalisation** of the scheme, presenting a step-by-step view of the accreditation journey for a specific technology. This includes applicant screening, ABA, IPT, and ongoing monitoring. For this phase, we refer to these sequential steps as *'Stages'*.

The third phase focuses on the **maintenance** of the scheme, outlining the *Tasks* required to ensure its continued effectiveness over time. It primarily involves repeating activities from the establishment Phase.

The approval and publication of the minimum standards of accuracy by the SoS will take place before any of the phases outlined above. This is a precondition for progressing with subsequent activities, as it provides the clarity needed to inform decisions on governance, timescales, and other key design elements of the accreditation process.

Phase 1: Establishment

We identified 8 tasks needed to set up the accreditation scheme, which can be grouped into 3 areas. Unless otherwise stated, all tasks described below are considered essential to the establishment of the scheme. Where an element is optional, this is clearly indicated within the relevant task description.

Area	Tasks
Governance	Task 1. **Design operating structure**: Define the TOM[3] including governance and oversight functions, a delivery roadmap with key milestones and timeframes, and roles and responsibilities necessary to manage and deliver the scheme. Conduct an internal capacity assessment to identify gaps and establish necessary capabilities via new hires and/or upskilling initiatives.
	Task 2. **Appointment of assessors conducting screening, ABA and/or IPT**: Identify and appoint suitable parties (Ofcom internal teams or third-party assessors) responsible for conducting the accreditation activities. This process includes sourcing potential candidates, defining required skills and qualifications, evaluating their competencies, and - when third-party assessors are involved - establishing formal legal agreements, as well as approving and setting up the scope and parameters of third-party involvement.
	Task 3. **Training of assessors conducting screening, ABA and/or IPT**: Provide training to individuals (Ofcom internal teams or third-party assessors) responsible for conducting accreditation activities. This task is essential to support consistency and impartiality across the accreditation process.
Technical infrastructure	Task 4. **Identify technical infrastructure needs**: Define and document the systems and capabilities required to support applicant screening, ABA, IPT and associated data management. This involves (1) for application screening, identifying the service requirements for the application submission portal and webpage, and conducting a Data Protection Impact Assessment ('DPIA') where personal data is processed; (2) for ABA, identifying the hosting infrastructure requirements for

[3] Target Operating Model: Strategic blueprint that defines how an organisation operates to deliver on its business objectives. See OC&C Strategy Consultants, Fundamentals of the Target Operating Model, 2025.

	data collected, and developing a data retention policy, along with a DPIA if required; and (3) for IPT, sourcing potential candidates as data providers, hosting infrastructure providers, and testing environments; identifying technical service requirements; establishing data governance and security protocols; assessing hosting infrastructure options; and developing a data acquisition plan and agreement.
	Task 5. **Obtain testing data (IPT only):** Identify, obtain access to multiple relevant datasets, and select stratified sub-samples to prepare suitable testing datasets. This involves acquiring data from providers, conducting legal reviews, establishing agreements with data partners, and, where required, transferring data from third-party providers to the hosting infrastructure, setting up data storage, and performing preprocessing tasks such as annotation, labeling, and anonymisation.
	Task 6. **Prepare Technical Environment** <u>Build, borrow, or buy the application submission platform:</u> Develop a secure, user-friendly submission portal to manage the full application lifecycle, either by building it in-house or procuring it from an external provider. This includes identifying the core features of the portal, conducting UX/UI work to design the interface and site structure, creating a landing page for submissions, hosting the portal in a secure live environment, testing it with stakeholders, and optimising usability and functionality. The portal will serve as the primary interface between applicants and Ofcom. <u>Build, borrow, or buy ABA infrastructure:</u> Develop a secure infrastructure to ingest, store, and manage commercially sensitive data for ABA, either in-house or via a secure third-party host. This includes strict access controls, audit trails, and clear data retention policies, with contractual safeguards to protect intellectual property and confidentiality. <u>Build, borrow, or buy a secure testing environment (IPT only):</u> Establish a secure environment to support IPT, either by building it in-house or procuring it from an external provider. In addition to the considerations above, this also includes developing the infrastructure needed to host test datasets and run IPT processes, setting up agreements with appropriate lab or server providers, and completing any necessary security and compliance checks.
Minimum standards of accuracy	Task 7. **ABA Assessment Rubric:** Develop an assessment rubric aligned with the minimum standards of accuracy published by the SoS. This will include a set of questions mapped to each

	objective, guiding applicants on the evidence required and ensuring a consistent approach to scoring by the assessors.
	Task 8. **Thresholds for IPT:** Develop the testing protocols for the IPT and determine and implement the benchmarked thresholds using the mechanism approved and published by the SoS. These thresholds will be based on the results of IPT from the 'previous testing period'. In the first instance, the thresholds will be set based on the performance of the first round of technologies that pass the ABA.

Phase 2: Operationalisation

We identified 13 stages required to run the accreditation scheme, which can be grouped into 4 areas. Unless otherwise stated, all stages described below are considered essential to the operation of the scheme. Where an element is optional, this is clearly indicated within the relevant stage description.

Area	Stages
Pre-launch / Launch	Stage 0. **Launch the scheme**: Officially announce and launch the accreditation scheme, including publishing scheme documentation, opening the application portal, and communicating key timelines and requirements to applicants. This could also include launching a marketing campaign to raise awareness of the scheme and developing and publishing supportive toolkits and services.
Applicant screening	Stage 1. **Invite potential applicants**: Following the launch of the accreditation scheme, invite relevant technology providers (via email and/or open calls on the official website) to submit applications for accreditation.
	Stage 2. **Applicants apply for accreditation**: Interested technology providers prepare and submit their applications, including the completed 'Application Cover Sheet' along with all required documentation and supporting information.
	Stage 3. **Screening assessor reviews applications**: Conducts an initial review of submissions to verify completeness and check eligibility.
	Stage 4. **Screening assessor determines eligibility and issues invitation to ABA**: Based on the initial review, formally invite eligible applicants to proceed to the ABA stage. Screening assessors could provide ineligible applicants with a clear rationale, and an appeal process could be introduced to

	allow applicants to contest these decisions; however, this is considered optional in the current scheme design.
Audit-based assessment (ABA)	Stage 5. **Assign ABA assessor for the assessment:** Assign qualified individuals or specific teams to conduct the ABA. Where the ABA is outsourced, applicants should be informed of the assessors involved.
	Stage 6. **ABA assessor receives information**: Receive the completed ABA questionnaire and all required supporting documentation from the applicant, as specified in the application guidance.
	Stage 7. **ABA assessor conducts assessment**: Score the applicant's technology against the ABA rubric, which assess the four principles ('Technical Performance', 'Fairness', 'Robustness', and 'Maintainability')' and their associated objectives and questions.
	Stage 8. **Issue approval or rejection**: Based on the result of the ABA, the assessor issues an approval scoring at least 50/100 on each of the four principles and at least 60/100 on the total aggregated score, to proceed to IPT (based on Ofcom's proposal published in December 2024). Applicants who do not meet these thresholds will receive a rejection letter. ABA assessors could provide unsuccessful applicants with a clear rationale, and an appeal process could be introduced to allow applicants to contest these decisions; however, this is considered optional in the current scheme design.
Independent performance testing (IPT)	Stage 9. **IPT assessor confirms declared category**: Confirm the specific testing category under which the technology will be tested for accreditation.
	Stage 10. **IPT assessor gets the technology**: Request and obtain access to the applicant's technology for testing purposes. This could be done via containerisation for technologies that can be used to tackle CSEA content, or via containerisation or secure APIs for technologies that can be used to tackle terrorism content.
	Stage 11. **IPT assessor conducts testing against test data**: Conduct performance testing using pre-defined datasets in a secure testing environment. This involves configuring a testing suite (including both illegal and benign data), conducting the tests, obtaining and recording the results. Before formal testing, a pre-testing inspection could be carried out to assess the technology's readiness by verifying that it can

	interface correctly with the test environment, operate under the specified test conditions, among other checks.
	Stage 12. **Issue approval or rejection**: Upon successful testing, the assessor issues an approval if the technology meets or exceeds the defined IPT thresholds, or a rejection if it does not. Passed technologies will be added to Ofcom's catalogue of accredited technology, and referenced in Ofcom's annual report under section 128 of the Act. IPT assessors could provide unsuccessful applicants with a clear rationale, and an appeal process could be introduced to allow applicants to contest these decisions; however, this is considered optional in the current scheme design.
Ongoing monitoring during application screening, ABA, and/or IPT	Stage 13. **Ongoing monitoring and review of assessors conducting screening, ABA, and/or IPT activities**: Regular review of the decisions made by assessors (Ofcom internal teams or third party) conducting screening, ABA and/or IPT to ensure objectivity and consistency in scoring. This activity is not mandatory but is recommended to support quality assurance and accountability across the scheme.

Phase 3: Maintenance

We identified 8 tasks required to maintain and continuously improve the accreditation scheme. These activities are grouped into 4 areas. Unlike earlier phases, most tasks in this phase are not essential but are recommended or optional, depending on their specific role in supporting the scheme over time. The table indicates the expected frequency of each task, distinguishing between ongoing and periodic activities.

Areas	Stages / Tasks	Frequency
Governance	Task 2. **Re-appointment of assessors conducting screening, ABA and/or IPT**: Conduct periodic reviews of parties (Ofcom internal teams or third party) responsible for conducting accreditation activities. Where needed, appoint new assessors. While not mandatory, this task is recommended to ensure assessors continue to meet required standards over time.	Periodic
	Task 3. **Re-training of assessors conducting screening, ABA and/or IPT**: Provide periodic or updated training to individuals (Ofcom internal teams or third-party assessors) responsible for	Periodic and Ongoing

	conducting accreditation activities. Re-training of assessors conducting accreditation activities is highly recommended to ensure they remain up to date with scheme requirements and maintain good practice. This is key to promoting consistency, impartiality, and alignment with evolving standards and processes. Ongoing training is also recommended to reinforce and refresh assessor knowledge, and to support their continued development.	
Technical infrastructure	Task 4. **Maintenance of the application submission platform**: Maintain the application platform. This may involve technical upkeep, IT upgrades, support, licensing, and ongoing improvements. Ongoing platform maintenance is essential to ensure the scheme remains operational and accessible to applicants.	Ongoing
	Task 5. **Maintenance of testing data**: Maintain the testing data, which may include renewing contracts and licences with data providers, ongoing dataset updates, and data storage maintenance. This task is essential to ensure IPT can be delivered reliably, remains aligned with legal and technical requirements, and stays responsive to evolving threats and content patterns.	Ongoing
	Task 6. **Maintenance of the secure testing environment:** Maintain the testing environment, which may include regular system updates, performance and security monitoring, managing infrastructure availability, resolving technical issues, and renewing contracts with service providers as necessary to support IPT testing operations. Maintaining this environment is essential for the secure and continuous operation of IPT.	Ongoing
Minimum standards of accuracy	Task 7. **ABA assessment rubric**: Periodically review and update the assessment rubric and associated questions to keep them current and relevant. Regular review is highly recommended and considered good practice to ensure the audit process remains relevant, consistent, and aligned with evolving standards and harms.	Periodic

	Ofcom may also periodically review the underlying objectives to consider whether they remain fit for purpose, providing further advice to the SoS if changes may be appropriate.	
	Task 8. **Thresholds for IPT**: Update and publish the thresholds against which technologies are tested, using the results of IPT from the 'previous testing period,' in line with the mechanism approved and published by the SoS. Periodic review is essential to ensure thresholds remain evidence-based and reflect current technical capabilities.	Periodic
Ongoing monitoring and review	Task 9. **End-of-period scheme review and evaluation**: Conduct an end-of-period scheme review, including process and impact evaluations, to assess the effectiveness of the scheme's implementation and determine whether it is achieving its objectives. While not mandatory, this activity is recommended to support continuous improvement and inform future policy or operational adjustments.	Periodic

While **re-accreditation** is not in scope for this work, we recognise that a process for periodic reassessment may be necessary to ensure ongoing compliance and performance of accredited technologies. This needs to be developed at a later stage, subject to future policy decisions, such as the accreditation validity period and the applicable minimum standards.

4.2 Governance Arrangements

Governance arrangements will be essential to ensure the scheme's independence, accountability, and operational effectiveness. Governance design will determine how Ofcom exercises oversight, how third-party roles are structured, appointed, and monitored, and who is responsible for delivering each part of the scheme.

4.2.1 Key Governance Responsibilities

Accreditation schemes typically involve a set of governance functions to uphold process integrity and ensure credible, effective decisions. Scheme responsibilities regularly include six core responsibilities:

1. **Set the standards:** Develop the standards that technologies must meet to achieve accreditation. This responsibility typically sits with the public

authority or scheme owner.[4] In this scheme, the SoS is responsible for setting minimum standards of accuracy as set out in the Online Safety Act.

2. **Develop the scheme:** Develop detailed accreditation criteria in line with the standards set out above, and scheme documents, as well as the overall design of the accreditation scheme, including objectives, milestones and timescale, eligibility rules, assessment procedures, and the required skills, experience, and qualifications for assessors. This function typically sits with the scheme owner.

3. **Approve the scheme:** Review and formally approve the scheme to ensure alignment with the standards and regulatory requirements. This function is typically performed by the public authority. In this scheme, Ofcom holds overall accountability for its delivery and operation.

4. **Appoint assessors:** Determine the suitability of the assessors and appoint assessors who are competent to conduct assessments in accordance with scheme criteria. This function is typically performed by the scheme owner or the public authority, depending on the delivery model. In other schemes, assessors are often accredited by the United Kingdom Accreditation Service (UKAS) against standards, such as ISO 17065, to ensure they are competent to carry out assessments. This provides formal recognition of the assessor's competence and involves regular compliance reviews to ensure continued adherence to the requirements.

5. **Conduct assessment:** Carrying out the technical evaluations of applicant technologies or services against the scheme's criteria and issuing accreditation decisions.

[4] The **scheme owner** refers to the organisation responsible for designing, maintaining, and overseeing the high-level rules, standards, and governance of an accreditation or certification scheme.

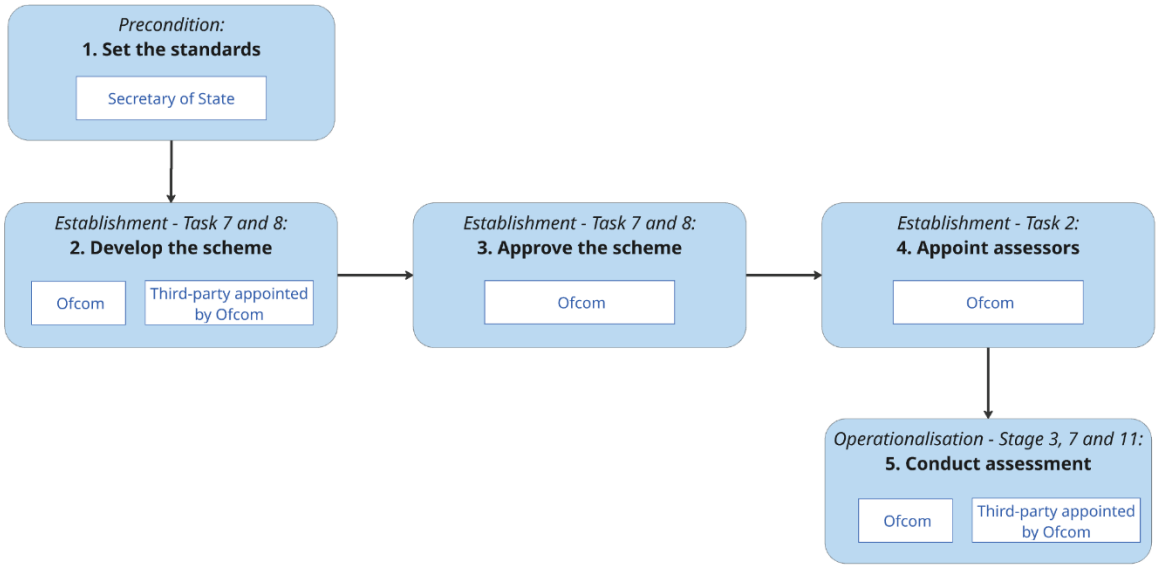


Figure 1 – Governance responsibilities and corresponding Tasks or Stages

In practice, governance models vary in how these responsibilities are divided between the regulator and third-party partners, particularly in the degree of operational involvement the regulator retains.

The governance model will determine Ofcom's level of operational involvement in delivering the accreditation scheme. We have identified a range of governance options for Ofcom, from minimal oversight to full in-house delivery, reflecting different levels of regulatory control, operational involvement, and resource commitment.

	Option 1 **Minimal Oversight**	**Option 2** **Scheme Owner I**	**Option 3** **Scheme Owner II**	**Option 4** **In-house**
Ofcom's Roles	3 and 4	2, 3, and 4	2, 3, and 4	2, 3, 4 and 5
Description	Ofcom outsources scheme development to a third party and appoints them as assessors. The third party acts as both the scheme owner and assessor. Ofcom has a limited role, providing oversight and	Ofcom outsources scheme development to a third-party contractor but retains scheme ownership. Ofcom appoints one or more third-party assessors to conduct accreditation.	Ofcom develops the scheme internally with peer review As in Option 2, Ofcom acts as the scheme owner. Ofcom appoints one or multiple third-party assessors to conduct the accreditation.	Ofcom develops the scheme internally with peer review and acts as the scheme owner. Ofcom appoints its own staff as assessors to conduct the accreditation.

	approving the scheme.			

4.2.2 Lean vs Formal Models

To simplify the range of governance options, we group delivery models into two overarching approaches: a **Lean Model** for early implementation and a **Formal Model** for a more mature scheme. This framework provides Ofcom with flexibility to adjust its level of operational involvement over time, balancing internal delivery and external outsourcing as the scheme evolves.

Our analysis suggests the Lean Model offers the most proportionate and practical starting point, enabling Ofcom to launch the scheme quickly while maintaining robust regulatory oversight. As the scheme matures, Ofcom could retain flexibility to transition towards a Formal Model, expanding external delivery to support long-term scalability and efficiency.

Lean Model

The Lean Model is a streamlined approach focused on quick implementation, with operational responsibilities absorbed into Ofcom's existing business-as-usual (BAU) functions wherever possible. Most operational activities (e.g., applicant screening, ABA, IPT, and ongoing scheme management) would be delivered internally, reducing the need for extensive external contracting.

This model is intended to support a 'Day 1' launch, enabling Ofcom to establish the scheme rapidly with lower external costs, but requiring greater internal staffing capacity. While this approach places more pressure on internal teams, it minimises contractual complexity and allows for faster mobilisation.

Formal Model

The Formal Model offers a more structured and externally delivered approach, aligned with standardised accreditation practices. Under this model, Ofcom retains core oversight but outsources key operational functions, such as assessor approval, training, and assessments, to one or more qualified third-party providers. This reduces day-to-day internal resource demands but leads to higher upfront project and procurement costs.

The Formal Model is envisaged as a 'future-state' option, suitable for a more mature scheme with stable demand and formalised delivery processes.

4.2.3 Delivery Model Options

As part of this feasibility study, we also examined potential delivery models for the scheme, acknowledging that decisions on delivery approach will directly shape the design and sequencing of process stages.

Broadly, we identified **three potential delivery models for the scheme,** which could be operated, either by Ofcom itself or in collaboration with third-party organisations:

1. Fully outsourced to a single or multiple third-party bodies
2. Partially outsourced to one or multiple third-party bodies
3. Fully managed in-house by Ofcom

Each delivery model presents trade-offs in operational control, complexity, and resource burden. A fully outsourced model may offer efficiency and scalability but lacks a clear candidate with end-to-end capability, particularly for IPT. A fully in-house model would maximise control but impose significant setup and operational demands. A modular, partially outsourced approach appears the most practicable: it offers flexibility to tailor delivery responsibilities, supports legal and operational safeguards for high-risk content, and reflects stakeholder preferences for Ofcom to retain a visible oversight role. The analysis below sets out the detailed considerations of each model.

Fully outsourced model

One option we explored is a **fully outsourced model**, where all aspects of the accreditation scheme would be delivered by third-party organisations, either through a single provider managing the entire process or multiple providers handling separate components.

A single-provider approach would involve Ofcom appointing one organisation to deliver the accreditation scheme in full, covering all stages from application screening through to final decision-making. An example of a comparable structure is the Age Check Certification Scheme, where the Information Commissioner's Office ('ICO') appointed the ACCS to conduct assessments. However, this approach appears unlikely to be suitable in this context. Based on our research, we did not identify any single organisation that currently appears to possess the full range of capabilities and infrastructure required to deliver the scheme end-to-end, particularly in relation to IPT, which involves access to both CSEA and terrorism data and secure testing environments.

A more modular outsourcing model would involve allocating different components of the process (i.e. applicant screening, ABA, and IPT) to capable specialist providers where they exist. In some cases, a single provider could cover more than one element, for example both applicant screening and ABA. While this approach could allow more targeted use of technical expertise and reduce reliance on any single provider, it would also introduce additional complexity for Ofcom, including greater coordination needs, more intensive quality assurance, and more complex contractual arrangements.

Interviews with potential applicants indicated no objection in principle to specialist third-party delivery, provided providers were demonstrably independent. However, there was a slight preference for Ofcom to retain a more active delivery role, reflecting its status as an independent and trusted regulator.

Partial outsourcing model

We also considered a modular, partially outsourced model, where Ofcom retains overall responsibility for the accreditation scheme but decides, on a component-by-component basis, whether to deliver specific elements in-house or delegate them to trusted third parties. This flexible approach allows Ofcom to align delivery with its internal capacity, legal obligations, and strategic priorities, while maintaining clear oversight of all accreditation activities. Below, we outline potential delivery arrangements for each core component.

Applicant screening could be delivered either by Ofcom or a third party. Any third-party provider would need to securely store and handle potentially large volumes of applications, including commercially sensitive information.

ABA could similarly be delivered in-house or outsourced. Third-party providers would need the technical capability to securely manage sensitive materials and the operational capacity to recruit, train, and oversee qualified assessors. Formal agreements would be required to govern data handling and audit criteria.

IPT is the most complex component, particularly due to the legal sensitivities around datasets. Delivery options would likely vary by harm type (CSEA or terrorism), raising two key considerations:

1. *Which party/parties would host the testing data?*

   A range of hosting configurations is possible. Ofcom could host both illegal and benign datasets, only one of these, or a subset of each. For example, Ofcom could host and validate benign data directly while managing the sub-sampling of datasets to protect the secrecy and security of testing materials, supporting transparency and control during early pilots or tightly governed deployments. Another option is a third-party model, where trusted external partners host and manage both benign and illegal datasets. This may reduce Ofcom's operational burden but would require robust oversight. A hybrid model may offer the most practical balance at scale: for example, Ofcom could manage benign data while third parties handle illegal content, especially CSEA, given the legal restrictions and associated risks. This approach could best balance transparency, control, and legal defensibility. Determining the most appropriate model will depend on further legal analysis, infrastructure readiness, and the intended delivery model for accreditation.

When it comes to CSEA content, secure databases of relevant material, including hashes, images, videos, text, and URLs are already maintained by designated UK authorities and legally authorised partners. Access and handling of this content is tightly restricted under UK law. Under the Protection of Children Act 1978 ('PCA 1978')[5] and the Criminal Justice Act 1988 ('CJA 1988'),[6] offences such as possession, making, and distribution of indecent images of children are generally prohibited. However, certain organisations, such as law enforcement and designated safeguarding bodies, are permitted to handle this material under specific statutory defences, including Section 46 of the Sexual Offences Act 2003.[7] A Memorandum of Understanding ('MoU') between the Crown Prosecution Service ('CPS') and the National Police Chiefs' Council ('NPCC') provides further clarification on how such defences should be applied in practice.[8]

Ofcom and its direct partners benefit from a more recent legal provision under Section 214(1) of the Online Safety Act 2023,[9] which establishes a statutory defence that permits the 'making' of indecent images of children when strictly necessary for online safety functions, including accreditation. The courts have interpreted 'making' broadly - for instance, in Atkins v DPP; Goodland v DPP [2000] 2 Cr. App. R. 248,[10] the Court of Appeal held that it includes downloading, saving, or even opening a file that results in temporary storage on a device.[11] Section 214 therefore enables Ofcom and those engaged by Ofcom (or assisting it in the exercise of any of its online safety functions) to legally handle CSEA content. While the statutory defence in Section 214 of the Online Safety Act 2023 does not extend to other offences such as possession or distribution, it is a defence to those offences where the person had a 'legitimate reason' for possessing or distributing the material.

For terrorism content, available datasets tend to be more limited. While some sources exist, such as UK and international hash databases maintained by industry coalitions or specialist organisations, the overall infrastructure is more fragmented. Unlike CSEA, where illegal material is clearly defined and centralised, terrorism content involves greater legal and contextual ambiguity. Definitions vary across jurisdictions, and

[5] legislation.gov.uk, Protection of Children Act 1978
[6] legislation.gov.uk, Criminal Justice Act 1988
[7] legislation.gov.uk, Sexual Offences Act 2003
[8] CPS, Memorandum of Understanding Between the Crown Prosecution Service (CPS) and the National Police Chiefs' Council (NPCC) concerning Section 46 Sexual Offences Act 2003, 2022
[9] legislation.gov.uk, Online Safety Act 2023
[10] BAILII, England and Wales High Court (Administrative Court) Decisions. ATKINS v. DIRECTOR OF PUBLIC PROSECUTIONS v. GOODLAND v. DIRECTOR OF PUBLIC PROSECUTIONS [2000] EWHC Admin 302 (8th March, 2000), 2000
[11] Crown Prosecution Service, Cybercrime - prosecution guidance, 2024

available datasets may include material that does not meet the definition of terrorism under UK law. As a result, content may fall into legal grey areas depending on ideology, intent, or political expression. These factors, combined with the absence of a known, standardised or government-backed dataset infrastructure, limit the availability of comprehensive terrorism datasets suitable for IPT.

2. *Which party/parties would host the testing environment?*

For CSEA data, hosting the testing environment requires careful navigation of legal, operational, and security requirements.

A key consideration is whether hosting must occur on-premises or whether secure cloud deployments could be permitted. While UK Government policy promotes a 'Cloud First' approach, encouraging public sector organisations to adopt cloud services and modernise legacy systems, it also recognises that alternative models may be appropriate in specific contexts.[12] The extreme sensitivity and criminal nature of CSEA content introduce unique complexities. Public cloud services are typically designed to meet the OFFICIAL threat model (including SENSITIVE), but CSEA content - while not formally classified as SECRET or TOP SECRET - may require equivalent protections due to its sensitivity and the need for high-integrity handling.[13] Consequently, although cloud hosting is not legally prohibited, its use in this context would require exceptionally rigorous safeguards. Other accreditation scheme operators and testing dataset owners highlighted the necessity for tightly restricted, role-based access with full auditability; robust encryption at rest, in transit, and during upload; careful consideration of data location; clearly defined retention and deletion policies compliant with UK GDPR; and formal agreements ensuring that all handling is proportionate and necessary. These requirements align broadly with the NCSC's Cloud Security Principles.[14] Despite the technical feasibility of secure cloud deployments, many stakeholders view on-premises environments as preferable for CSEA testing, given their clearer legal defensibility, stronger security assurances, and more direct operational control.

Another consideration is whether CSEA content used in testing environments should be subject to a UK residency requirement. While there is no universal mandate for government data classified as OFFICIAL

[12] Government Digital Service and Central Digital and Data Office, Guidance. Government Cloud First policy, 2023
[13] NCSC, Guidance. Cloud security guidance. Service and deployment models
[14] NCSC, Guidance. Cloud security guidance. The cloud security principles

(including SENSITIVE) to be physically hosted within the UK,[15] departments are expected to take risk-based decisions on offshoring, including assessing where data is stored, who manages the infrastructure, and who can access it.[16] For example, the Ministry of Justice does not routinely require UK-only hosting, provided that appropriate legal, data protection, and security measures are in place.[17] However, guidance also notes that some datasets carry heightened security risks and warrant consultation with departmental security teams.[18] Given the criminal status and exceptional sensitivity of CSEA content, some stakeholders recommend UK-only hosting. This approach helps mitigate risks associated with cross-border legal conflicts, foreign access obligations, and international data transfers.[19] It also facilitates clearer evidential processes for criminal investigations, simplifies compliance with UK GDPR, and supports the high standards of security, integrity, and auditability expected under CPS guidance.[20]

For terrorism and benign content, hosting arrangements may be more flexible. As with CSEA datasets, testing environments could be hosted by either Ofcom or a trusted third-party provider, provided the necessary legal defences and safeguards are in place. The key difference is that terrorism and benign datasets are generally subject to fewer specific statutory restrictions and operational safeguards than CSEA, offering a wider range of lawful options for where and how the data is hosted. The choice of hosting model would still depend on legal considerations, infrastructure capabilities, and the ability to manage operational and security risks, including compliance with data protection laws, clear legal agreements, and the capacity to support secure, scalable, and cost-effective testing, either on-premises or in the cloud.

Fully managed in-house by Ofcom

Lastly, we considered a model in which Ofcom would deliver the entire accreditation process in-house. This approach would offer the highest levels of control, accountability, and operational consistency, but would also require significant investment in infrastructure, technical expertise, and staffing capacity.

Ofcom would need to establish or procure secure testing environments and fully resource the end-to-end accreditation process. This model would likely involve

[15] Government Digital Service, Guidance. Multi-region cloud and software-as-a-service, 2025
[16] Government Digital Service, Government Commercial Function and Central Digital & Data Office, Guidance. Cloud guide for the public sector, 2023
[17] Ministry of Justice, Security Guidance. Data sovereignty
[18] Government Security, Principle: B3 Data Security
[19] Information Commissioner's Office, A guide to international transfers, 2025
[20] Crown Prosecution Service, Disclosure Manual: Chapter 30 - Digital Material, 2022

longer implementation timelines, higher operational costs, and could face significant barriers to securing access to datasets, particularly CSEA material, without offering clear and significant advantages over a partially outsourced approach.

4.3 Details of Each Task and Stage

This section breaks down each individual stage of the accreditation process, providing a more detailed explanation of what happens at each step. It explains the specific tasks within each stage, their purpose, key activities, and any decision points, as well as practical considerations such as inputs, outputs, and dependencies.

4.3.1 Phase 1: Establishment

This phase sets out the foundational components needed to establish the accreditation scheme, covering three key areas: **Governance**, **Technical Infrastructure**, and **Minimum Standards of Accuracy**. Each area is broken down into specific tasks designed to ensure the scheme is credible, effective, and operationally ready.

1. **Governance**

Governance is one of the three core areas within the Establishment phase of the accreditation scheme. It refers to the **design of structures, roles, and oversight mechanisms** that ensure the scheme's credibility, accountability, and operational effectiveness.

It determines who delivers core accreditation functions, such as ABA and IPT, how responsibilities are allocated between Ofcom and third-party providers appointed by Ofcom, and how assurance is maintained throughout the life of the scheme. Decisions at this stage will have a lasting influence on the scheme's independence, transparency, and long-term effectiveness.

Core Tasks

As outlined above, governance involves **three core tasks**:

- Task 1. Design operating structure
- Task 2. Appointment of assessors conducting screening, ABA and/or IPT
- Task 3. Training of assessors conducting screening, ABA and/or IPT

While defining the operating structure (Task 1) and appointing delivery parties to conduct assessments (Task 2) are essential to the scheme's functioning, training assessors (Task 3) is highly recommended. This reflects the reality that in more informal delivery models, individuals, whether internal staff or external parties, may not always receive formal training. While training is strongly encouraged to ensure consistency, impartiality, and quality, it may not be required in every delivery configuration, particularly where roles are absorbed into BAU functions.

In such cases, alternative measures, such as peer review or periodic checks of assessments, could help ensure consistency and quality of decisions.

Why This is Important

Stakeholders consistently emphasised four governance principles: **independence, transparency, a smooth user experience, and opportunities for meaningful engagement**. Embedding these principles, especially in the scheme's early stages, is likely to strengthen public confidence and support operational resilience.

Stakeholders also highlighted the importance of **adaptability**. As the scheme scales or evolves, Ofcom may need to revisit delivery arrangements, strengthen oversight, or respond to changes in the legal and technological landscape. Early governance decisions should avoid locking the scheme into rigid models, leaving space to adapt, whether by onboarding new partners, updating assurance methods, or responding to regulatory developments.

Delivery Model Considerations

Decisions about delivery will determine how responsibilities are allocated between Ofcom and external partners, with direct implications for operational feasibility, public trust, and overall scheme effectiveness.

Some governance tasks, such as *designing the operating structure (Task 1)*, must be delivered in-house to align with Ofcom's statutory duties. *Appointing delivery partners (Task 2)* is also expected to remain internal in the initial Lean Model but as the scheme matures, Ofcom could choose to appoint an external delivery partner as assessors, rather than relying on internal teams. *Training (Task 3)* offers greater flexibility, with the option to deliver it internally or outsource depending on capacity and delivery preferences.

Stakeholders highlighted clear trade-offs. **Internal delivery** provides stronger oversight and can reinforce perceptions of independence but would require significant investment in specialist expertise, secure infrastructure, and staffing, raising questions about Ofcom's ability to attract and retain the necessary talent, particularly given private sector salary competition.

Outsourcing could ease resourcing pressures but increases risks related to impartiality, quality assurance, and market capacity. Stakeholders raised concerns about the limited pool of technically credible and independent organisations, noting that many experts already work for large platforms or technology vendors. These risks underscore the need for strong safeguards, including transparent appointment criteria, regular audits, independent complaints mechanisms, and clear separation between oversight and delivery roles.

Finally, whether the scheme is delivered by Ofcom or by a third party appointed by Ofcom, a phased approach could be considered, initially limiting the scope of accreditation, for example by prioritising specific technologies or content types. This could help manage operational capacity and support a more controlled implementation. The decision would fall within Ofcom's discretion to define the scheme's scope and focus, and could be revisited as delivery processes and capacity matures.

Assets Required

Where Ofcom appoints a third party to conduct assessments, delivering governance functions effectively will require **access to technically capable, demonstrably independent partners** able to conduct assessments and manage sensitive data securely. Technical capability may be assessed through prior experience conducting audits or evaluations in comparable sectors, completion of approved training, demonstrated proficiency in handling high-risk data, and the ability to meet defined performance and security benchmarks. Independence could be evidenced through transparent governance arrangements and operational separation from assessed providers, where relevant.

Any delivery partners must operate within strict legal and operational safeguards, particularly for CSEA content, where legal restrictions tightly control who can lawfully handle such material. As explained earlier, Section 214 of the Online Safety Act 2023 provides Ofcom and its authorised partners with a statutory defence for making illegal content when strictly necessary for online safety functions, including accreditation.

Maintaining high standards of security, legal compliance, and independence will remain essential to securing public and industry trust. These may include ISO 27001 certification (or equivalent), adherence to the NCSC's Secure Design Principles, demonstrable compliance with UK GDPR,[21] and independent oversight or audit mechanisms. In practice, the number of suitable partners is still expected to be limited given the sensitivity of the data and the strict handling requirements.

2. Technical Infrastructure

Technical infrastructure is one of the three core areas within the Establishment phase of the accreditation scheme. It refers to the **systems, tools, and processes** required to enable secure, efficient, and legally compliant delivery of accreditation activities, particularly for application screening, ABA, and IPT.

Establishing the right infrastructure - one that is both applicant-friendly and responsive to the differing needs of technologies and data types - is key to the

[21] legislation.gov.uk, Regulation (EU) 2016/679 of the European Parliament and of the Council, 2025

scheme's credibility, effective delivery, and compliance with legal and technical safeguards. It determines how Ofcom and/or delivery partners access, store, process, and safeguard sensitive commercial information and illegal content throughout the accreditation lifecycle. Early decisions in this area will shape the user experience, data security, and long-term operational flexibility of the scheme.

Core Tasks

As outlined above, technical infrastructure involves **three core tasks**:

- Task 4. Identify technical infrastructure needs
- Task 5. Obtain testing data
- Task 6. Prepare technical environment

These tasks are all essential due to their foundational role in scheme delivery, ensuring the systems and resources are in place for secure, effective, and compliant operation. Task 4 focuses on defining the infrastructure requirements for applicant screening, ABA, and IPT, including service needs, hosting environments, and security protocols. Task 5, which applies specifically to IPT, covers the acquisition and preparation of appropriate testing datasets, including legal agreements, secure transfers, and data processing. Task 6 involves building or procuring the applicant portal, ABA infrastructure, and establishing secure testing environments for IPT, ensuring operational readiness for both application handling and technical assessments.

Why This is Important

Technical infrastructure is critical to the scheme's security, legal compliance, and operational effectiveness by enabling each stage (i.e., applicant screening, ABA, and IPT), to be carried out in a secure, efficient, and legally defensible way. For example, screening requires a secure portal for application intake and document handling; ABA requires infrastructure that can securely manage proprietary documentation while supporting consistent and auditable assessment processes; and IPT may require fully managed environments capable of safely and securely handling illegal content. Weak infrastructure at any of these stages could expose sensitive data, compromise the fairness or consistency of assessments, and diminish stakeholder confidence in the scheme's integrity.

A simple and intuitive online portal is essential for **applicant screening**. Stakeholders consistently stressed the importance of a user-friendly interface, transparent processes, and responsive support to encourage participation. For **ABA**, the secure handling of commercially sensitive data at scale requires robust infrastructure, featuring strict access controls, comprehensive audit trails, and clear data retention policies. However, key trade-offs must be managed: enforcing standardised formats can improve assessment efficiency but may limit flexibility for diverse technologies, while retaining records to ensure auditability

must be balanced against applicants' expectations around data minimisation and intellectual property protection.

IPT presents the most complex infrastructure requirements. Testing environments must comply with legal restrictions on handling terrorism and CSEA content. Potential accreditation users also noted that they should support diverse deployment formats (e.g., containerised models, APIs) and varied compute needs (e.g., from CPUs to GPUs) to ensure accuracy, flexibility, and fairness. Potential applicants further stressed the importance of tailored datasets for different tool types (e.g., hash-matching versus AI classifiers) to enable meaningful and accurate evaluation.

A well-designed technology stack should also anticipate long-term operational needs, including re-accreditation, dataset updates, and structured record-keeping to ease repeat applications. Updates to IPT datasets were considered necessary over time to maintain relevance and accuracy as threats evolve.

Delivery Model Considerations

Decisions on infrastructure delivery will directly shape how the scheme's systems are built, maintained, and scaled over time. Ofcom will need to determine which elements to deliver in-house and which to outsource, with implications for operational resilience, legal compliance, and delivery timelines.

Task 4 must be delivered in-house to align with Ofcom's statutory responsibilities and oversight role. *Tasks 5 and 6* could be delivered internally or outsourced, depending on legal constraints and resource capacity.

- **Applicant screening**: Ofcom could either develop the applicant submission portal internally or contract a specialist provider. Whichever option is chosen, the portal must meet high standards for accessibility (e.g., Web Content Accessibility Guidelines ('WCAG') 2.2 compliance), security (e.g., ISO 27001-aligned controls), and data protection (e.g., UK GDPR).[22] Internal development would require ongoing management of applicant queries, submission tracking, and service performance monitoring, potentially increasing staffing and training needs.
- **ABA**: ABA requires secure infrastructure to ingest and store commercially sensitive data, which could be managed via internal systems or secure third-party hosting. Stakeholders were open to submitting detailed evidence but stressed the need for legal safeguards to protect intellectual property and confidential data. Third-party hosting would need robust contractual terms, including audit rights, access control guarantees, policy retention policies, and liability limitations.

[22] legislation.gov.uk, Regulation (EU) 2016/679 of the European Parliament and of the Council, 2025

- **IPT**: IPT presents the greatest legal and technical complexity. The sensitivity of CSEA content limits viable delivery partners, with a strong practical preference for on-premises environments. While cloud options are not legally ruled out, their use would require robust safeguards - such as strict access controls, end-to-end encryption, and careful consideration of data location - as outlined in the Section 4.2.3 Delivery Model Options.

  If Ofcom does not establish its own facility, formal agreements would be needed with authorised bodies that already benefit from statutory defences under UK law, or with contractors who could operate under Ofcom's extended legal cover, as described earlier. While Section 214 of the Online Safety Act 2023 introduces a statutory defence for Ofcom employees and authorised contractors engaged in online safety functions, including accreditation, this may broaden the pool of eligible partners only to a limited extent. In practice, the number of suitable partners is still expected to remain small due to the sensitivity of the data and the strict handling requirements. Stakeholders also noted that the combination of legal, operational, and security constraints will continue to significantly limit viable options. While there is no definitive list, likely candidates include public bodies with existing statutory mandates to handle CSEA content, as well as highly secure contractors operating under Ofcom's legal defence. Stakeholders also noted that the combination of legal, operational, and security constraints will continue to significantly limit viable options.

  For terrorism and benign data, cloud or hybrid models may offer greater flexibility. In all cases, formal agreements with data holders will be essential to govern access, ingestion, labelling, and maintenance of datasets.

  There are three broad delivery models for running IPT, each with distinct legal, operational, and infrastructure implications:

  - **Fully outsourced model**: A third party manages the entire testing environment and conducts evaluations. This option is scalable and requires less internal infrastructure, but may raise legal, security, and oversight challenges, particularly for CSEA content.
  - **Endpoint model**: Applicants access test datasets via a secure API and run evaluations within their own environments. This mirrors real-world deployment and reduces Ofcom's infrastructure burden but introduces risks around data protection, consistency of evaluation conditions, and - in the case of CSEA content - significant legal and safeguarding concerns.
  - **Managed environment model**: Ofcom hosts and controls the testing environment and conducts all evaluations in-house. This model offers the highest level of control and assurance, especially for

CSEA content, but entails greater operational complexity and higher setup and running costs.

In practice, different delivery models may be more suitable depending on the type of content. A managed environment may be most appropriate for CSEA datasets, given their legal and safeguarding requirements, while more flexible approaches may be sufficient for terrorism and benign datasets.

Assets Required

Delivering technical infrastructure will require a combination of secure IT systems, specialised infrastructure, and trusted data partnerships to ensure compliant and effective scheme delivery. Key assets include:

- **Application submission platform**: A secure, user-friendly portal to manage applications, documentation, and applicant queries. This includes front-end web interfaces, back-end data management systems, and secure cloud or on-premises hosting.
- **ABA infrastructure**: Secure environments for ingesting, processing, and storing commercially sensitive information, with strong access controls, audit logging, encryption (where appropriate), and clear data retention policies.
- **IPT testing environment**: High-security environments capable of handling terrorism and CSEA datasets, with flexibility to support multiple deployment formats (e.g., containerised models, APIs) and compute configurations (e.g., CPU, high-memory GPU setups, and clustered GPUs for larger models). This includes secure data storage, compute resources, and system monitoring.
- **Data partnerships**: Formal agreements with relevant data holders (e.g. for CSEA, terrorism, and benign datasets) to secure lawful access to testing datasets. These partnerships should define the terms of access, ingestion, update cycles, and any usage limitations.
- **Internal legal and governance safeguards:** Internal frameworks to govern how sensitive data is handled once accessed. This includes legal agreements, evidence handling protocols, data minimisation practices, access logging, and demonstrable compliance with UK data protection and criminal law requirements, alongside training and wellbeing support for personnel handling distressing material.

3. Minimum Standards of Accuracy

Minimum standards of accuracy are one of the three core areas within the Establishment phase of the accreditation scheme. This area covers the

development of an ABA assessment rubric aligned with the minimum standards of accuracy, the **implementation of benchmarked thresholds** using the mechanism approved and published by the SoS, alongside the development of IPT testing protocols.

The SoS's approval and publication of the minimum standards of accuracy, which includes the objectives and minimum score for passing the assessment against these objectives, as well as the mechanism for calculating the applicable thresholds, will take place before these tasks begin. This step is an **essential precondition** for proceeding.

Clear minimum standards are essential to ensure the scheme operates fairly, consistently, and with sufficient rigour to promote safe and effective technology use. These standards underpin the integrity of the accreditation process, providing potential applicants with transparency on expectations and enabling Ofcom to make defensible, evidence-based accreditation decisions.

Core Tasks

As outlined above, setting the minimum standards of accuracy involves **two core tasks**:

- Task 7. ABA assessment rubric
- Task 8. Thresholds for IPT

Both tasks are essential to the effective operation of the scheme, as they provide the legal and operational foundation needed to assess applicant technologies. Without them, the scheme would not be able to function.

Why This is Important

Besides being a statutory requirement, clear and publicly available minimum standards of accuracy are fundamental to the scheme's credibility and legitimacy. They ensure that all applicants are assessed against consistent, transparent, and objective criteria, promoting trust among applicants, industry, and the wider public.

Delivery Model Considerations

Responsibility for setting minimum standards of accuracy rests with the SoS, as mandated by the Online Safety Act.

Based on these standards, Ofcom's role will be to operationalise them, whether this is in-house or through a specialised third party, developing the necessary assessment rubrics, including assessment procedures and eligibility rules.

Under the Lean model, Ofcom would be expected to take on this role internally during early implementation phases. As the scheme matures, outsourcing

elements of scheme development could become a more practical and scalable option.

Assets Required

Delivering this area effectively will require:

- Formal documentation of minimum standards set by the SoS and assessment rubrics;
- Internal capacity within Ofcom to translate standards into operational ABA and IPT procedures if done in-house;
- Governance mechanisms to review and update operational criteria in line with any changes issued by the SoS;
- Public-facing materials to ensure transparency and accessibility of accreditation requirements.

4.3.2 Phase 2: Operationalisation

The following sections outline the key broad stages required to operationalise the accreditation scheme, starting with Stage 1 (Applicant Screening). A preceding Stage 0 (Launch the scheme) covers the pre-launch and launch of the scheme itself. While Stage 0 is not part of the formal accreditation flow, it is a critical enabler for Stage 1 and is therefore addressed there as part of the operational setup.

1. Applicant Screening

Applicant screening is the first of the four broad operational stages within the accreditation process. It covers the **initial interaction between applicants and Ofcom (or its appointed delivery partner)**, including application submission, eligibility check, and communication of outcomes. The purpose of this stage is to ensure that only applicants meeting published eligibility criteria proceed to the ABA phase.

This stage also incorporates key setup activities from Stage 0, such as launching the application portal and applicant support services, publishing guidance materials, and issuing invitations to apply. Submitted applications undergo an eligibility check, with a potential appeal process where appropriate. While procedurally straightforward, this stage is essential for establishing the process and enabling uptake.

Core Stages

As outlined above, application screening involves **four core stages**:

- Stage 1. Invite potential applicants
- Stage 2. Applicants apply for accreditation
- Stage 3. Screening assessor reviews applications
- Stage 4. Screening assessor determines eligibility and issues invitation to ABA

These stages are essential to the scheme, as they provide the essential starting point for the accreditation process. They establish a clear entry pathway, ensuring the scheme operates in an orderly and transparent way from the beginning. An appeal process could be introduced to allow applicants to contest eligibility decisions.

Why This is Important

The applicant screening stage serves as a critical **initial filter, ensuring that only applicants who meet the published eligibility criteria progress** to the more resource-intensive stages of accreditation. This helps manage operational demands, protects the integrity of the process, and ensures that applicants are subject to a fair, consistent entry mechanism.

As the first point of contact between applicants and the scheme, this stage also plays a key role in shaping perceptions of seriousness, transparency, and accessibility. Stakeholders consistently emphasised the importance of clear communication, responsive support, and opportunities for feedback. In particular, smaller and early-stage providers expressed concerns that a one-time, binary decision could unfairly exclude viable technologies due to minor documentation errors or misunderstandings. Interviewees highlighted the importance of mechanisms to clarify or supplement applications, viewing this as key to ensuring fairness and avoiding unintended exclusions.

Additionally, stakeholders stressed the value of early-stage guidance, including accessible materials and a responsive support function to assist applicants, particularly those with fewer resources or less familiarity with accreditation processes. Investing in user-friendly application systems and clear, accessible guidance can reduce applicant friction, improve submission quality, and ultimately enhance efficiency throughout the accreditation process.

Delivery Model Considerations

Applicant screening involves a set of administrative, technical, and procedural tasks that **could be delivered internally by Ofcom or outsourced** to a trusted third party. Key functions include operating the application portal, checking eligibility, communicating outcomes, and, if adopted, managing a feedback or appeal process.

Delivering **screening in-house** would provide Ofcom with direct control over applicant engagement, eligibility decisions, and quality assurance - an approach well-suited to a Lean Model, particularly in the early phases of implementation. However, this model would likely require more investment in staffing, operational workflows, and digital systems to manage application intake, case management, and applicant support.

Alternatively, **some or all screening functions could be outsourced**, offering potential operational efficiencies, especially if integrated with later stages such as ABA. Partial outsourcing could involve a third party managing the application portal and conducting initial eligibility checks, while Ofcom retains responsibility for final decisions, oversight, and applicant communications. Regardless of the model, any outsourcing arrangement would require robust contractual safeguards, clear escalation procedures, and strong oversight mechanisms to ensure accountability, data protection, and consistent applicant experience.

While stakeholders expressed no strong preference on the delivery model, they consistently stressed the importance of transparent communication and accessible support, regardless of delivery model.

Assets Required

Effective applicant screening will require:

- Accessible application materials and toolkits, including eligibility guidance, submission templates, and FAQs tailored to different applicant profiles.
- A secure, user-friendly online portal for application submission, ideally offering status tracking and integrated applicant support.
- Applicant support services, such as a helpdesk or dedicated contact point, to answer queries and assist applicants, particularly those unfamiliar with accreditation processes.
- Eligibility review capacity, whether in-house or contracted, with trained assessors applying consistent criteria.
- Case management systems to monitor application progress, manage queries, and document decisions.

In addition, Ofcom may consider implementing an appeals process or other feedback mechanisms to ensure fairness and provide pathways for applicants to clarify or correct submissions. These features are optional and could be introduced depending on the final scheme design.

By combining these assets with clear operational processes, Ofcom can maximise scheme accessibility, improve applicant experience, and maintain a fair and efficient accreditation process.

2. Audit-Based Assessment (ABA)

ABA is the second of the four operational stages within the accreditation process. It involves the structured evaluation of applicant technologies against the minimum standards of accuracy set by the SoS, using submitted documentation and technical evidence. The purpose of the ABA is to evaluate evidence relating to a technology's performance, development and maintenance in order to assess whether it can deliver accurate, reliable, and sustainable detection outcomes.

This stage encompasses issuing audit questions, reviewing applicant submissions, scoring against a defined rubric, and communicating results. Where adopted, it could also include an appeals or feedback mechanism. The ABA serves as a critical quality control step within the accreditation scheme, and determines which technologies proceed to IPT, if IPT is included within the scheme's final design.

Core Stages

As outlined above, ABA involves **four core stages**:

- Stage 5. Assign ABA assessor for the assessment
- Stage 6. ABA assessor receives information
- Stage 7. ABA assessor conducts assessment
- Stage 8. Issue approval or rejection

All four stages are critical to delivering a rigorous and fair accreditation process. The only optional component is the appeals process, which - if implemented - would be incorporated within Stage 8, providing unsuccessful applicants with a clear rationale for rejection and the opportunity to challenge decisions.

Collectively, these stages establish a transparent, structured mechanism for evaluating the readiness and quality of applicant technologies, serving as a key quality checkpoint before progression to subsequent stages (such as IPT, if adopted).

While not a formal part of the accreditation process itself, Ofcom has a legal obligation to report annually on its use of the Technology Notice power, including any technologies accredited under the scheme. This requires Ofcom to publish a list of technologies that have been successfully accredited, although there is no obligation to disclose individual assessment results or identify unsuccessful applicants.

Why This is Important

The ABA stage is **central to the integrity of the scheme**, providing the mechanism for determining whether applicant technologies satisfy the minimum standards of accuracy set by the SoS (with or without IPT). It requires applicants to provide robust evidence demonstrating how their technology meets specific objectives, which is then evaluated by Ofcom or a nominated third party to assess whether the minimum standards set by the SoS have been met.

Potential accreditation users widely agreed on its importance but cautioned that, if poorly designed, it could become an overly bureaucratic barrier, particularly disadvantageous to smaller or resource-constrained providers. Across interviews, providers called for a **transparent, flexible, and interactive process.** Several urged Ofcom to avoid 'black box' assessments and instead offer clear guidance, feedback loops, and opportunities to clarify or amend submissions. Many

favoured draft submissions or iterative evidence packages, allowing the process to assess the technology itself rather than applicants' administrative capacity. However, this approach would significantly increase resource demands, requiring substantial staff time for feedback, queries, and reviews. Delivering this effectively may also necessitate a secure portal or case management system to support iterative submissions and differentiated applicant journeys.

There was also demand for **clarity on scoring criteria and outcomes**. While some providers supported publishing the ABA scores achieved against the minimum standards of accuracy to enhance transparency, others expressed concern about reputational risks if data lacked appropriate context. Several recommended offering applicants a preview or opportunity to challenge their scores before final decisions.

Concerns about administrative burden, particularly for smaller companies, were widespread, with many advocating for a **streamlined assessment process**. One proposed approach was to recognise existing third-party certifications (e.g., ISO 27001, ISO/IEC 23053) to reduce documentation requirements. This would require Ofcom or its delivery partner to define accepted certifications, establish equivalence rules, and implement verification processes.

Finally, stakeholders emphasised the need for **adaptability and proportionality**. Assessment frameworks should evolve alongside technology developments, with mechanisms for updating templates, retraining assessors, and incorporating feedback. One interviewee noted, for example, that a tool achieving 97% accuracy might be acceptable for a smaller service with active human moderators, but inadequate for a large-scale platform where a 3% error rate could result in significant harm. This highlights how the same performance metric can carry different implications depending on scale and risk.

Delivery Model Considerations

Delivering the ABA stage involves a labour-intensive process requiring the review of sensitive documentation, including technical specifications, development processes, validation reports, and accuracy metrics. Ofcom will need to decide whether to manage these assessments **in-house or outsource** them to specialist providers.

Regardless of the model chosen, robust systems, trained personnel, and clear operational procedures will be essential to ensure assessments are impartial, consistent, and legally compliant. This decision will have significant implications for operational complexity, resource requirements, and the scheme's scalability.

In-house delivery would offer Ofcom greater oversight and control over quality assurance but would require substantial investment in skilled assessors, secure systems, and case management infrastructure. These demands would increase

further if appeals mechanisms were included, as staff may need to revisit decisions, document rationales, and engage directly with applicants to resolve disputes. This approach may be more feasible in the early phases but could present challenges as demand grows.

Outsourcing to accredited third-party assessors could offer greater scalability and cost efficiencies by leveraging existing expertise, infrastructure, and flexible staffing models, particularly if integrated with other stages of the scheme. However, given the commercially sensitive nature of the technologies, this approach would require clear legal and contractual arrangements, covering scope, security, and disclosure obligations, as well as robust governance mechanisms to ensure consistent assessment quality and maintain public trust.

Assets Required

Effective delivery of ABA will require a combination of technical systems, qualified personnel, and robust operational processes:

- Secure document submission and management systems, capable of handling sensitive commercial and technical data.
- Trained auditors, with expertise in technical evaluation, risk assessment, and regulatory compliance, either within Ofcom or contracted externally.
- An ABA assessment rubric that translates the minimum standards of accuracy into clear, weighted scoring criteria, enabling consistent evaluation across all applications.
- Flexible case management systems, able to track iterative submissions, applicant queries, and appeals.
- Protocols for including recognised third-party certifications (e.g., ISO 27001, ISO/IEC 23053) where appropriate as accepted evidence to be factored into the ABA assessment, thereby reducing applicant burdens without compromising assessment rigour.
- Clear applicant-facing guidance and support, including feedback mechanisms to ensure transparency throughout the process.

By investing in these assets, Ofcom can ensure that ABA upholds scheme credibility while remaining accessible and proportionate for a diverse range of applicants.

3. Independent Performance Testing (IPT)

IPT is the potential third stage of the operationalisation phase within the accreditation scheme. It involves a structured evaluation of applicant technologies under controlled conditions, following successful completion of the ABA stage. The primary objective of IPT is to independently assess performance in standardised, representative testing environments, designed to be representative of real-world use cases.

IPT is a technically and legally complex stage, requiring secure testing environments, clearly defined performance metrics, and carefully curated datasets tailored to each technology type. Ofcom will need to determine whether to formally incorporate IPT within the accreditation process.

Core Stages

As outlined above, IPT involves **four core stages**:

- Stage 9. IPT assessor confirms declared category
- Stage 10. IPT assessor gets the technology
- Stage 11. IPT assessor conducts testing against test data
- Stage 12. Issue approval or rejection

If formally included within the accreditation process, all four stages would be essential to verify technology performance, serving as the final quality assurance checkpoint before accreditation. The only optional component is the appeals process, which - if implemented - would be integrated into Stage 12, providing unsuccessful applicants with clear reasons for rejection and the opportunity to appeal.

IPT independently tests technologies against representative datasets and conditions, mitigating reliance on self-reported data and verifying performance in realistic deployment contexts. This strengthens trust and assurance in accredited tools among regulators, platforms, and end-users, and can inform decisions on whether their use should be required in a Technology Notice.

Why This is Important

Potential accreditation users stressed that IPT must evaluate **how technologies perform in their intended operational settings** - considering specific threat environments, use cases, and deployment conditions - rather than applying generic testing. A one-size-fits-all approach was seen as inappropriate, potentially producing misleading results and undermining scheme credibility.

A consistent theme across interviews was the need for **clarity and transparency**: applicants should understand what is being tested, how performance is measured, and how results are interpreted. **Dataset quality and maintenance** was a primary concern, with stakeholders emphasising that testing data should reflect real-world and emerging threat types, include detailed labelling across relevant categories (e.g., CSEA, benign, synthetic adult content), and be regularly updated to remain relevant. Several providers warned that poorly constructed datasets, such as those containing outdated, mismatched, or irrelevant material, could produce misleading scores and undermine the credibility of the process. To mitigate this, Ofcom would need to partner with trusted entities to source and curate testing datasets, and establish a governance framework to manage how data is selected, labelled, updated, and maintained over time.

Providers also emphasised the importance of **testing under deployment conditions representative of real-world use** (e.g., cloud infrastructure, APIs, or edge devices) to ensure fairness and avoid penalising tools outside their intended context. This would require Ofcom or delivery partners to replicate diverse deployment environments and support smooth integration.

In general, stakeholders supported several **key design features for IPT**:

- Right-of-reply mechanisms, allowing applicants to make minor fixes or request re-testing in cases of anomalies linked to testing setup.
- Performance banding, providing contextualised results by deployment context (e.g., low-power devices versus cloud), helping users interpret performance appropriately.
- Provisions for continuous improvement, such as periodic or incremental re-testing to accommodate model updates without requiring full re-accreditation.

Without these features, stakeholders worried that IPT risks disincentivising participation, particularly among smaller or more innovative providers.

Delivery Model Considerations

Delivering the IPT stage involves key decisions around legal permissions, dataset handling, deployment setup, and result communication. Ofcom will need to determine **which elements to deliver in-house and which could be outsourced** to trusted third parties, while accounting for important legal and operational constraints.

CSEA content presents the most stringent legal requirements as only a limited number of entities have historically been legally permitted to hold or process this material, effectively ruling out testing models such as endpoint testing. However, under Section 214 of the Online Safety Act 2023, legal defences are extended to Ofcom and authorised contractors assisting with Ofcom's online safety functions. This provides greater flexibility to appoint delivery partners who can lawfully handle CSEA data for accreditation purposes. Nonetheless, the handling of CSEA datasets will continue requiring secure, controlled environments - whether hosted by Ofcom or authorised partners - alongside robust safeguards to ensure lawful processing, data security, and public trust. Applicants would be expected to submit their technology and deployment instructions for testing within these secure environments.

By contrast, **terrorism and benign datasets** are not subject to the same statutory restrictions as CSEA content, offering greater flexibility in delivery models, including the possibility of endpoint testing or API-based evaluations within applicants' own infrastructure. However, both still require careful handling, due to

the harmful nature of terrorism content and the need to comply with UK GDPR and other legal and regulatory requirements.

Assets Required

Delivering IPT effectively will require a combination of secure infrastructure, specialist personnel, and well-defined operational processes. Core assets include:

- High-quality, regularly updated datasets, including sensitive CSEA and terrorism content, as well as representative benign datasets, maintained in line with legal requirements and evolving threat profiles.
- Legally compliant, high-security testing environments, either on-premises or cloud-based, with robust cybersecurity protections.
- Ongoing infrastructure maintenance and operational oversight, including technical capacity to set up, run, and monitor tests, as well as to deploy and securely remove applicant technologies from the testing environment.
- Sufficient skilled technical personnel, with expertise in integration, troubleshooting, and test execution across diverse deployment models.
- Applicant support and engagement mechanisms, including helpdesks or dedicated contact points.
- Governance frameworks to oversee dataset updates, manage appeals (where relevant), ensure testing fairness, and maintain consistency and transparency across cycles.

4. Ongoing monitoring and review during application screening, ABA, and/or IPT

Ongoing monitoring and review of the decisions made by the individuals or teams responsible for delivering accreditation activities, specifically those conducting applicant screening, ABA, and IPT, constitutes the final stage of the operationalisation phase. This stage supports continuous quality assurance, early risk detection, and alignment across assessors and delivery partners.

Proactive monitoring helps maintain fair and consistent assessments, reinforces trust in outcomes, and safeguards the overall integrity of the scheme.

Core Stages

As outlined above, the ongoing monitoring during application screening, ABA, and/or IPT involves **one core stage**:

- Stage 13. Ongoing monitoring and review of assessors conducting screening, ABA, and/or IPT activities

While not formally mandatory, this stage is considered good practice and is recommended to uphold quality, accountability, and compliance across the scheme.

Why This is Important

Active oversight ensures that assessors and delivery partners' decisions apply standards consistently and follow updated procedures. Without it, delivery may become uneven, outcomes less transparent, and public confidence undermined. Regular performance review of these decisions enables Ofcom, or a nominated delivery partner, to detect and address issues early.

Scheme operators emphasised the value of structured compliance mechanisms. These include maintaining assessor capabilities through continuous professional development (CPD), establishing formal channels to report and investigate complaints or whistleblowing disclosures, and drawing on real-world intelligence, such as user feedback, reported breaches, or certification results, as inputs for audit and refinement.

Delivery Model Considerations

This function could be managed **internally by Ofcom or delegated** to a trusted third party. In either case, the responsible body should be equipped to collect performance data, review individual cases, and respond to procedural deviations. Monitoring can be embedded into workflow reporting and supplemented by audits or spot checks as needed.

Assets Required

Delivering this stage effectively is likely to require:

- Performance and compliance monitoring frameworks, including criteria to evaluate assessor conduct, procedural adherence, and case outcomes.
- Governance mechanisms to raise concerns, trigger reviews, and implement remedial actions.
- Expert oversight capacity, such as independent reviewers or quality assurance leads to support evaluation and calibration.

4.3.3 Phase 3: Maintenance

Phase 3 sets out how the accreditation scheme could be maintained and improved over time following its initial establishment. This phase comprises 8 tasks, grouped into five areas: (1) **Ongoing monitoring and review**, (2) **Governance**, (3) **Technical infrastructure**, (4) **Minimum standards of accuracy**, and (5) **Ongoing monitoring and review**.

Each area includes specific activities intended to ensure the scheme remains effective, proportionate, and responsive to evolving technologies and threats.

Core Activities

Key areas and associated activities include:

- **Governance**, which involve 2 core tasks:

    - Task 2. Re-appointment of assessors conducting screening, ABA and/or IPT
    - Task 3. Re-training of assessors conducting screening, ABA and/or IPT
- **Technical infrastructure**, which involve 3 core tasks:
    - Task 4. Maintenance of the application submission platform
    - Task 5. Maintenance of testing data
    - Task 6. Maintenance of the secure testing environment
- **Minimum standards of accuracy**, which involve 2 core tasks:
    - Task 7. ABA assessment rubric
    - Task 8. Thresholds for IPT
- **Ongoing monitoring and review**, which involves 1 core task:
    - Task 9. End-of-period scheme review and evaluation

Unlike earlier phases, most tasks in this phase are not mandatory but are considered recommended or optional, depending on their role in maintaining the scheme over time. By contrast, maintenance of the technical infrastructure (tasks 4, 5, and 6) is essential. These tasks ensure the scheme remains functional and accessible to applicants, that IPT can be delivered securely and reliably, and that infrastructure continues to meet legal, technical, and security requirements as threats evolve. For this reason, these tasks should be delivered on an ongoing basis.

Periodic review of the ABA assessment rubric and the IPT thresholds is also strongly encouraged. In particular, updating IPT thresholds is considered essential and, under current proposals, would occur every 4 years using results of the 'previous testing period,' in line with the mechanism set by the SoS. This ensures thresholds remain evidence-based and responsive to advances in detection capabilities.

Most tasks in this phase should be carried out periodically, typically at the end of an accreditation cycle or the beginning of a new one. Under the proposed model, this would occur every four years. However, some stakeholders suggested that tasks relating to assessment criteria (i.e. ABA assessment rubric and IPT thresholds), may warrant annual review to keep pace with updated evaluation practices and technological developments.

Stakeholders also recommended that individuals delivering screening, ABA, and/or IPT undergo re-training on a regular cycle, potentially annually, to keep pace with evolving standards, technologies, and procedural changes. Ongoing professional development was seen as important to ensure staff remain up to date. Any material changes to the scheme would likely necessitate retraining across delivery teams and partners.

Why This is Important

Potential accreditation users emphasised the value of **regular, scheme-wide reviews** to ensure that accreditation processes, standards, and test datasets remain aligned with technological advances and emerging risks. Periodic consultation with technical experts and delivery partners was viewed as an important way to maintain credibility, inform updates, and ensure the scheme remains responsive and effective over time.

Delivery Model Considerations

Activities in Phase 3 could be carried out by **Ofcom, a third-party partner, or a combination of both**. For example, technical infrastructure may be maintained by internal teams or through contracted providers, while periodic activities, such as scheme reviews or re-training, could be supported by external experts. Regardless of the delivery model, it will be important to ensure clear roles, coordination, and oversight to maintain continuity and uphold quality standards over time.

Assets Required

Delivering this stage effectively would likely require:

- Governance processes for periodic scheme review, including datasets, and audit rubrics.
- Expert advisory capacity, including access to technical and sector specialists to inform scheme updates, emerging threats, and alignment with evolving industry standards.

The preceding sections of this report detailed all activities required within a single accreditation cycle. By contrast, Phase 3 focuses on maintaining and updating components already in place. While this phase is expected to carry lower overall costs than scheme establishment, certain tasks, particularly infrastructure maintenance and dataset renewal, may introduce ongoing or recurring cost drivers. These should be factored into long-term planning and resourcing decisions.

4.3.4 Re-accreditation

While not a formal stage or within the scope of this feasibility study, re-accreditation is widely recognised as an important mechanism to ensure that accredited technologies continue to meet minimum standards over time. Its core function is the periodic reassessment of accredited tools to verify sustained performance in light of evolving threats andtechnical updates.

Re-accreditation involves reassessing applicants after initial certification to confirm ongoing compliance with scheme standards. This is particularly relevant for tools that rely on retrainable models or incorporate machine learning, where

performance may degrade over time or drift due to changes in data, use cases, or operational environments.

Why This is Important

Stakeholders broadly supported the need for **regular re-accreditation** to maintain confidence in the long-term effectiveness of accredited technologies. Without periodic review, there is a risk that tools deviate from their originally accredited state or fail to address emerging risks.

At the same time, stakeholders highlighted the importance of **balancing assurance with proportionality**. Requiring full re-accreditation on a fixed annual basis, or mandating complete documentation re-submission for minor updates, was seen as potentially burdensome, particularly for smaller providers with limited resources, and could discourage participation.

Many recommended mechanisms for **event-triggered reassessment**, where tools would be re-evaluated following significant updates, such as the release of a new version or a change in intended functionality. This could involve Ofcom proactively tracking material changes or requiring providers to notify and submit revised documentation when updates occur.

Delivery Model Considerations

Re-accreditation could be managed **internally by Ofcom or delegated** to a nominated third party. Regardless of the delivery model, the responsible body would need to maintain oversight of model changes, performance trends, and emerging risks to inform timely and proportionate reassessment cycles.

Assets Required

Delivering this stage effectively would likely require:

- Documentation retention systems, allowing secure, long-term storage of applicant submissions, assessments findings, and testing results to enable efficient re-assessment processes without requiring full re-submission.
- Monitoring mechanisms to track accredited technologies, model updates, and material changes impacting performance.
- Case management systems to ensure continuity and transparency in applicant records, reducing administrative burden during re-accreditation.

While re-accreditation is not in scope for this work, we recognise that a process for periodic reassessment may be necessary to ensure ongoing compliance and performance of accredited technologies. This could be developed at a later stage, subject to future policy decisions, such as the accreditation validity period and the applicable minimum standards.

5. Demand Modelling

5.1 Approach to Demand Modelling

The demand forecast for this accreditation scheme is a key element in the analysis, as the scheme's operational cost is influenced by the number of applications it receives. Specifically, operational expenses for BAU costs, the ABA and the IPT scale directly with the volume of applications. Consequently, an accurate demand projection is crucial for effectively understanding and managing the scheme's overall expenditures.

Our approach incorporates two distinct analyses:

- **Demand for Year 0:** This estimates companies that fall under the scope of this accreditation scheme, are capable of generating the necessary inputs for the initial accreditation process, and are willing to participate.
- **Demand for subsequent testing periods:** For each subsequent testing period, demand is estimated by adding:
    - Companies that failed to acquire accreditation in the immediately preceding period but are willing to reapply, and
    - New entrants that, since the last accreditation period, have developed the capacity to generate the necessary inputs for this accreditation process.

Companies whose products or services fall within the scope of this accreditation scheme and are capable of generating the necessary inputs are defined as the 'pool of possible applicants' for each specific period. The aforementioned capacity for applying or generating the necessary inputs for the accreditation application process is defined as a company's financial or structural ability to apply without requiring the development of new technologies or significant adaptations to existing ones. This translates to having the capability to develop the necessary inputs without extensively affecting their BAU operations (i.e., possessing a sufficient workforce to succeed in this process). We considered companies classified as small or larger to have the necessary capacity for this.

The demand used to estimate the final accreditation costs is derived from a model built upon a series of interconnected calculations, structured into distinct steps. The estimates are calculated by multiplying the initial pool of possible applicants by their willingness to apply.

Specifically, for the initial period (Year 0), the pool of possible applicants is defined as the number of companies capable of applying. For subsequent periods, conversely, the pool of possible applicants comprises both companies capable of applying and successfully completing the assessment, as well as those that applied but did not receive certification due to specific reasons. A comprehensive description of the demand modelling approach and the calculation steps can be found in the methodology section within the Appendix.

5.2 Estimated Demand of the Scheme

Based on the evidence gathered, our estimation indicates that **the initial pool of possible applicants consisted of 106 companies**. This figure represents the providers of technologies tackling CSEA and/or terrorism, are categorised within the targeted taxonomies for this accreditation process, and are capable of generating the necessary inputs during the ABA and the IPT. The estimated willingness to apply ranges from 51% to 73%, representing the lower and upper bounds of demand; further details are provided in the 'Willingness to Participate' section below.

Estimated Demand for Year 0	
Upper bound	61
Lower bound	42

In subsequent years, the demand for accreditation is estimated to fluctuate based on the number of new entrants applying and previously rejected applications. Our estimation is based on the expected growth rate of the international safety tech market, the assumed accreditation rate, and the willingness to reapply. Further details are provided in the section below.

Estimated Demand for subsequent testing periods	**Year 2**	**Year 4**
Upper bound	57	54
Lower bound	36	32

5.3 Evidence Base and Underlying Assumptions

5.3.1 Pool of Possible Applicants

In essence, the initial demand for Year 0 is projected as the product of the portions of the global safety tech population that already meet the scheme's technological and operational capacity requirements (pool of possible applicants) that are willing to apply. Following Year 0, the applicant estimation evolves. Future demand then encompasses both technologies that failed in previous periods but are willing to reapply, and newly developed technologies (after the prior testing period) that wish to participate.

Our estimation of demand is contingent upon technologies meeting both technological and capability requirements for participation in the accreditation scheme.

Technological requirements

Our assumption is that for a technology to be considered eligible, it must:

- Address the specific harms targeted by this accreditation scheme: CSEA and/or terrorism.
- Be categorised as the type of technology that Ofcom can require the use of in a Technology Notice. Specifically, these include: system-wide governance, platform-level, and age-oriented online [23].

The evidence is derived from 'The UK Safety Tech Sector: 2024 Analysis'[24] and the 'International State of Safety Tech 2024.'[25] Based on these sources, the proportion of companies addressing CSEA and/or Terrorism harms is 53.8%, while 49.0% of companies are considered part of the previously stipulated targeted online safety technology taxonomy.

Operational Capacity Requirements

Beyond technological alignment, companies need to have the operational capacity to meet the demands of the ABA. This includes preparing required documentation and responding in detail to the accreditor's queries. Organisations typically need either internal teams with the capacity to support this process or the resources to engage external support, ensuring minimal disruption to BAU operations.

We used the company size as a proxy of operational capacity. Companies classified as Small, Medium, or Large enterprises, drawing on definitions from 'The UK Safety Tech Sector: 2024 Analysis' by the Department for Science, Innovation and Technology ('DSIT')[26], were considered to meet the necessary operational capacity. Micro-businesses were excluded from this pool, as their operational scale is likely not able to support the engagement efforts required for the accreditation process. This assumption is based on interviews which indicated

[23] A full definition of the rest of the taxonomies is presented in the appendices.
[24] Department for Science, Innovation and Technology ('DSIT'), The UK Safety Tech Sector: 2024 Analysis, 2024
[25] Paladin Capital Group, International State of Safety Tech 2024, 2024
[26] According to the mentioned report, the company categories present the following characteristics: - Micro: Employees <10 and Turnover < €2m, or Balance sheet total < €2m.
- Small: Employees >10 and <50; and Turnover > €2m and < €10m, or Balance sheet total < €43m.
- Medium: Employees >50 and <250; and Turnover > €10m and < €50m, or Balance sheet total < €43m.
- Large: Employees > 250; and Turnover > €50m, or Balance sheet total > €43m.

that applying for accreditation would take substantial resources and capacity, which micro-businesses would not be able to provide. Additionally, we assume that some of these businesses will mature and grow, and thus be counted as a part of the demand modelling pool for future cycles of accreditation.

The foundational data informing these estimations, beyond the specific size definitions, is primarily derived from 'The UK Safety Tech Sector: 2024 Analysis' by the DSIT[27] and the 'International State of Safety Tech 2024'[28] reports. According to these reports, the proportion of companies that could be categorised as Small, Medium, or Large is 53.2%.

5.3.2 Willingness to Participate

A key variable in this model's estimation is the willingness to participate from the pool of possible applicants in each period. For Year 0, we considered the willingness to apply to be the same for all participants, as every company is new to this scheme. For subsequent periods, we applied the same willingness-to-apply estimate for new entrants, but used a different rate of willingness to reapply for companies that previously participated in the accreditation process and failed in the most recent testing period.

Willingness to Apply

The benchmark for the willingness to apply in Year 0 is based on interview data collected from a convenience sample of potential applicants to the scheme. Among the companies interviewed, 63% of the companies indicated they would be willing to apply to this scheme without any conditions, while 26% expressed interest but noted that certain conditions would need to be met. 9% of the companies stated they had no interest in participating.

To account for potential selection bias, the likelihood that more interested companies were overrepresented in the interview sample, we applied a conservative adjustment factor of 20%. This reflects the possibility that companies less engaged with the accreditation process may have opted out of the interview itself.

Given this, we provide a demand estimate as a range. The lower bound assumes only the unconditionally willing (63%) apply, adjusted downward by the 20% bias. The upper bound assumes all unconditionally willing companies apply, plus a portion of the conditionally willing group (89%), with the same bias adjustment. This yields an estimated Year 0 demand range of 51% to 73% of the pool of possible applicants.

[27] DSIT, The UK Safety Tech Sector: 2024 Analysis, 2024
[28] Paladin Capital Group, International State of Safety Tech 2024, 2024

Willingness to Reapply

For subsequent periods, we assume that 80% of applicants who have failed previously would be willing to reapply. This assumption is informed by two key sources: interviews with organisations offering comparable accreditation services, which suggest high levels of continued engagement, and the reaccredition rate of 89.2% in similar schemes[29], used here as triangulation to support long-term retention assumptions.

5.3.3 Accreditation Rate

Another key variable in this demand estimation for each period after the initial accreditation process is the accreditation rate, the proportion of applicants that successfully receive accreditation. This rate is critical for determining how many are rejected and therefore considered as potential applicants for the next accreditation cycle.

For modeling purposes, we adopt a conservative accreditation rate of 10%, based on Mechanism B outlined Ofcom's 2025 consultation[30], which defines IPT thresholds based on a percentile cut-off, and other government-backed technology accreditation schemes based on interviews conducted. Although conservative, this 10% benchmark is deemed plausible given the structure of the IPT and aligns with our assumption that many unsuccessful applicants will reapply due to minimal marginal costs after the initial submission.

[29]NCSC, Annual Review 2023, 2023
[30] Ofcom, Technology Notices to deal with terrorism content and/or CSEA content, 2024

6. Cost, Resourcing, and Timing Requirements

6.1 Overview

We estimated the cost, resource, and time requirements of the accreditation scheme, drawing from evidence collected via desk research, stakeholder interviews, and follow-up surveys. We developed two models to account for the complexity and variability in scheme implementation:

- **Lean model**: A streamlined version of the scheme intended for quick implementation, where responsibilities are absorbed into existing BAU functions wherever possible. This is likely to serve as the Day 1 model for the initial submission period (Year 0).
- **Formal model**: A more structured version of the scheme, aligned with standardised accreditation practices. This model represents the potential future state as the scheme matures.

For both models, we categorised costs into two groups:

- **BAU costs** refer to those associated with activities embedded within ongoing operations, requiring minimal additional overhead and no dedicated project structure (e.g., designing the operating structure).
- **Project costs** refer to those associated with activities requiring dedicated planning, resourcing, and governance, and which fall outside BAU delivery (e.g., acquiring and preparing training data). We adopted a modular approach to Project activities, aligned with the tasks and stages in the Progress Map. For each activity, we assessed both in-house and outsourced cost options. This modular structure allows individual components to be costed independently and flexibly combined, enabling users to model a range of delivery configurations.

6.2 Cost Modelling Summary

The cost estimation results are presented in 4 tables below, combining two costing models (Lean vs Formal Models) with different demand scenarios (low vs high demand). Each table reports minimum and maximum costs across:

- Hosting options: I.e., on premises and in the cloud
- Delivery models: I.e., in-house and outsourced
- Accreditation processes: I.e., ABA only, and both ABA and IPT

6.2.1 Estimated Costs

Year 0 costs include initial setup and the operational costs of the first round of technology testing during the initial submission period.[31] Net Present Value (NPV) costs cover all expenses from Year 0 to Year 4, including Year 0 costs, testing at Year 2 and Year 4, and maintenance for the first testing period.

The tables below present the Year 0 costs and the NPV for low-demand and high-demand scenarios for the Lean Model:

A. Low-demand scenario: Lean Model

LEAN MODEL		Cloud		On-Premise	
		Min Cost (£ thousands)	**Max Cost (£ thousands)**	**Min Cost (£ thousands)**	**Max Cost (£ thousands)**
ABA Only	**In-House**	Year 0 = 233.4 NPV = 484	Year 0 = 381.6 NPV = 643.3	N/A[32]	N/A
	Outsourced	Year 0 = 414.3 NPV = 936.5	Year 0 = 999.4 NPV = 1,815.4	N/A	N/A
ABA & IPT	**In-House**	Year 0 = 1,194.7 NPV = 2,019.7	Year 0 = 3,139.0 NPV = 4,267.2	Year 0 = 2,102.7 NPV = 2,634.4	Year 0 = 7,487 NPV = 81,38.8
	Outsourced	Year 0 = 1,634.3 NPV = 3,090.2	Year 0 = 4,187.5 NPV = 6,698.5	Year 0 = 2,542.3 NPV = 3,704.8	Year 0 = 8,535.5 NPV = 10,570

B. High-demand scenario: Lean Model

LEAN MODEL		Cloud		On-Premise	
		Min Cost (£ thousands)	**Max Cost (£ thousands)**	**Min Cost (£ thousands)**	**Max Cost (£ thousands)**
ABA Only	**In-House**	Year 0 = 273.8 NPV = 607	Year 0 = 422.1 NPV = 766.3	N/A	N/A
	Outsourced	Year 0 = 454.7 NPV = 1,059.4	Year 0 = 1,039.9 NPV = 1,938.3	N/A	N/A
ABA & IPT	**In-House**	Year 0 = 1,296.1 NPV = 2,328.1	Year 0 = 3,240.5 NPV = 4,575.6	Year 0 = 2,204.1 NPV = 2,942.8	Year 0 = 7,588.5 NPV = 8,447.1
	Outsourced	Year 0 = 1,701.7 NPV = 3,295.1	Year 0 = 4,254.9 NPV = 6,903.4	Year 0 = 2,609.7 NPV = 3,909.8	Year 0 = 8,602.9 NPV = 10,774.9

[31] Estimates reflect the present value of costs incurred from Year 0 to Year 4, which is considered as the first testing period. Net Present Value (NPV) is calculated using a standard discounting approach to account for the time value of money.

[32] In the 'ABA Only' scenario, Cloud and On-Premise hosting options present no mathematical difference between themselves as the IPT is not being delivered.

The tables below present the Year 0 costs and the NPV costs for low-demand and high-demand scenarios for the Formal Model:

A. Low-demand scenario: Formal Model

FORMAL MODEL		Cloud		On-Premise	
		Min Cost (£ thousands)	**Max Cost (£ thousands)**	**Min Cost (£ thousands)**	**Max Cost (£ thousands)**
ABA Only	**In-House**	Year 0 = 745.0 NPV = 1,263.6	Year 0 = 1,035.7 NPV = 1,840.1	N/A	N/A
	Outsourced	Year 0 = 856.8 NPV = 1,991.5	Year 0 = 1,813.6 NPV = 3,950.5	N/A	N/A
ABA & IPT	**In-House**	Year 0 = 1,697.1 NPV = 2,769.5	Year 0 = 3,786.4 NPV = 5,434.2	Year 0 = 2,605.1 NPV = 3,384.2	Year 0 = 8,134.4 NPV = 9,305.7
	Outsourced	Year 0 = 2,067.6 NPV = 4,115.3	Year 0 = 4,995 NPV = 8,803.8	Year 0 = 2,975.6 NPV = 4,730.0	Year 0 = 9,343 NPV = 12,675.3

B. High-demand scenario: Formal Model

FORMAL MODEL		Cloud		On-Premise	
		Min Cost (£ thousands)	**Max Cost (£ thousands)**	**Min Cost (£ thousands)**	**Max Cost (£ thousands)**
ABA Only	**In-House**	Year 0 = 824.2 NPV = 1,504.5	Year 0 = 1,114.9 NPV = 2,080.9	N/A	N/A
	Outsourced	Year 0 = 862.5 NPV = 2,008.6	Year 0 = 1,819.2 NPV = 3,967.6	N/A	N/A
ABA & IPT	**In-House**	Year 0 = 1,810.3 NPV = 3,113.8	Year 0 = 3,899.6 NPV = 5,778.5	Year 0 = 2,718.3 NPV = 3,728.5	Year 0 = 8,247.6 NPV = 9,650
	Outsourced	Year 0 = 2,073.3 NPV = 4,132.4	Year 0 = 5,000.6 NPV = 8,820.9	Year 0 = 2,981.3 NPV = 4,747.1	Year 0 = 9,348.6 NPV = 12,692.4

6.2.2 Cost Drivers

The total costs of delivering this accreditation would vary based on key policy and delivery decisions made by Ofcom. Below, we identify and analyse the four primary cost drivers:

1. **Inclusion of IPT.** Whether the accreditation scheme includes IPT would significantly impact the costs and resourcing required.
2. **Delivery model.** Costs vary depending on whether and to what extent delivery is managed by Ofcom in-house or outsourced.
3. **IPT hosting methods.** Hosting IPT on-premise or in the cloud carries different infrastructure and maintenance cost implications.

4. **Lean versus Formal Model.** The Lean Model involves streamlined processes and lower overheads, while the Formal Model entails more comprehensive governance, planning, and resourcing.

1. Inclusion of IPT

As outlined in the Process Map section, Ofcom has yet to decide on whether to recommend the inclusion of IPT in the minimum standards (and this is ultimately a decision for the SoS). However, the **method of IPT delivery** remains a critical factor in determining the overall cost of the scheme, due to its potential to significantly increase expenditure. This is primarily driven by the physical infrastructure costs, particularly if data storage and testing is hosted on-premise, and the acquisition of testing datasets.

The magnitude of these costs will vary significantly depending on Ofcom's decisions regarding delivery models and team structures. For example, all other factors being equal, including IPT could increase the total cost of the first testing periods (Year 0 to Year 4) by £1.5 to £5.0 million. These incremental costs specifically arise from data acquisition, increased staff hours and outsourcing services, and all associated maintenance and security costs related to hosting IPT and managing secure data.

2. Delivery Model (In-house or Outsourced)

Outsourcing accreditation delivery could raise the NPV by £450,000 to around £3.4 million, depending on whether those activities are delivered by the existing BAU team or by new, dedicated teams established specifically for this purpose. This cost differential is most pronounced in scenarios where only ABA is included in the process, as outsourcing is compared against a BAU cost increase. This increase represents the lowest magnitude cost within the model, particularly in the formal model's low-demand scenario and with on-premise storage.

3. IPT Hosting Method

The infrastructure for storing testing data and hosting the testing environment is a critical cost determinant, assuming IPT is delivered. An on-premise solution entails substantial upfront capital investment, estimated between £1 million and £4.5 million, for acquiring data centre infrastructure and establishing a secure testing environment. While cloud-based alternatives incur higher ongoing maintenance costs, these do not outweigh the significant upfront costs of physical infrastructure within the modelled timeframe. As a result, in the short to medium term, on-premise delivery leads to materially higher expenditure.

When compared to cloud infrastructure, opting for an on-premise solution could increase the NPV of the first testing period (Year 0 - Year 4) by between £615,000 and £3.9 million, depending on the investment scenario and whether the delivery model is structured as lean or formal.

4. Lean vs. Formal Model

The choice between a Lean and Formal delivery model represents another significant cost determinant in the accreditation process.

In the Lean model, most costs, particularly during the initial setup phase, are absorbed by the existing BAU team. While this makes it a cost-efficient option in the short term, BAU resource use becomes the primary ongoing cost in the model.

By contrast, the Formal model provides a more structured and scalable framework for accreditation delivery in later years. It includes additional costs for external validation, such as accreditation of potential assessors by UKAS. The model also incurs higher administrative overheads, including the appointment of assessors, scheme evaluation, and quality assurance processes.

Choosing the Formal model over the Lean model would increase the NPV of the first testing period (Year 0 to Year 4) by approximately £780,000 to £2.1 million, depending on the specific delivery scenario.

6.3 Lean Model

The Lean Model represents a streamlined version of the accreditation scheme, designed for quick implementation and early-stage delivery. It assumes that key responsibilities are absorbed into existing BAU functions wherever possible, minimising the need for new roles, systems, or governance structures. This model is particularly suited for the **initial submission period (Year 0)** and reflects a pragmatic 'Day 1' delivery approach.

It is intended to allow Ofcom to launch the scheme at pace, while deferring more complex or resource-heavy components, such as external accreditation or bespoke delivery systems to later phases of implementation.

6.3.1 Model Overview

Under the Lean Model, the delivery team is composed primarily of internal staff, who take on the responsibilities of scheme coordination, policy, operations, and technical assessment. These responsibilities are absorbed into existing structures where feasible, particularly when:

- The activity is generalisable (e.g., appointment of assessors, scheme review and evaluation)
- The task can be planned and trained in advance (e.g., ABA delivery, IPT design, approvals)

Wherever appropriate, responsibilities are consolidated across roles to reduce overhead and enable flexible deployment.

However, some actions would need to be **externalised** either:

- **Due to future** dependencies on third-party approvals (e.g., UKAS accreditation), or
- When scaling the scheme or responding to **high demand**, external delivery may become more cost-effective or operationally necessary.

A breakdown of BAU and Project activities under the Lean Model is provided below.

Lean Model	
BAU Activities	Design operating structure *(Task 1)*
	Appointment and re-appointment of parties conducting screening, ABA, and/or IPT *(Task 2)*
	Identify technical infrastructure need *(Task 4)*
	ABA *Assessment Rubric (Task 7)*
	Thresholds for IPT *(Task 8)*
	Delivery of application screening *(Stage 1, 2, 3, 4)*
	Delivery of ABA assessment *(Stage 5, 6, 7, 8)*
	Support of IPT delivery *(Stage 9, 10, 12)*
	Ongoing monitoring and review of the assessors *(Stage 13)*
	End-of period scheme review and evaluation *(Stage 13)*
Project Activities	Training and re-training of the assessors conducting screening, ABA, and/or IPT *(Task 3)*
	Obtaining testing data and the maintenance *(Task 5)*
	Build the application submission platform *(Task 6)*
	Build, borrow or buy a secure testing environment and the maintenance *(Task 6)*
	Launch the scheme *(Stage 0)*

	Delivery of IPT testing in a secure environment *(Stage 11)*

6.3.2 BAU Costs

With the IPT included in the accreditation process, the estimated BAU cost under the Lean Model is approximately £311,000 - £444,800 in Year 0, £218,700 - £319,100 in Year 2, and £204,500 - £308,500 in Year 4.

We considered two levels of resourcing: a **minimum viable team** and a **full-scale team**. The timesheet of each would depend on the scheme's assigned budget, the delivery risk tolerance, and demand expectations.

Minimum Viable Team

A breakdown of the roles of the minimum viable team is provided below.

Role	Role Description
Scheme Coordinator / Manager	Oversees the end-to-end delivery of the accreditation scheme. Manages daily operations, scheduling, documentation, and coordination across all functions. Acts as the main point of contact for internal stakeholders, applicants, and delivery partners. Leads on internal planning, reporting, and prioritisation.
Policy & Delivery Officer	Provides hands-on support across policy, operations, and administration. Manages applicant communications, meeting coordination, documentation, and assessment logistics. Supports scheme implementation by drafting guidance, maintaining internal processes, and ensuring smooth delivery across the team.
Assessor	Leads application review and ABA. Evaluates applicant submissions against eligibility and minimum standards. Provides evaluations, supports clarifications with applicants, and advises on improvements to assessment procedures. Collaborates with the IPT Technical Lead to ensure category alignment and, where relevant, supports interpretation of IPT results.
IPT Technical Lead	Leads the technical execution of the IPT process. Confirms the category of submitted technologies, designs and interprets test protocols, reviews model performance, and ensures alignment with technical standards. Owns the design of the IPT pipeline and ensures it meets scheme requirements.
Software Developer / DevOps Engineer	Develops and maintains software for the accreditation scheme, including applicant onboarding tools and assessment

	systems. Supports the IPT testing application, and manages automation and integration across the scheme's infrastructure.
Legal Advisor	Provides legal oversight on scheme design and implementation. Ensures compliance with the Online Safety Act, data protection legislation, intellectual property rights, and public procurement rules.

Full-Scale Team

A breakdown of the roles of the full-scale team is provided below.

Role	**Role Description**
Scheme Coordinator	Provides overall leadership and strategic oversight of the accreditation scheme. Coordinates cross-functional teams, sets priorities, and ensures delivery against objectives. Leads reporting to senior stakeholders and external bodies.
Scheme Manager	Manages the day-to-day operations of the accreditation scheme. Oversees scheduling, applicant tracking, documentation, and assessment logistics. Serves as the primary operational point of contact for internal teams and external applicants.
Policy & Delivery Officer	Supports the daily delivery of the accreditation scheme through hands-on operational and policy tasks. Manages applicant communications, schedules meetings, prepares documentation, and helps coordinate assessments. Provides administrative, analytical, and generalist support across onboarding, policy interpretation, and stakeholder engagement.
Policy & Delivery Officer	Supports the daily delivery of the accreditation scheme through hands-on operational and policy tasks. Manages applicant communications, schedules meetings, prepares documentation, and helps coordinate assessments. Provides administrative, analytical, and generalist support across onboarding, policy interpretation, and stakeholder engagement.
Assessor	Reviews applications for eligibility, completeness and suitability. Conducts ABA, reviewing documentation, governance processes, and claims.
IPT Technical Lead	Leads the technical planning and delivery of IPT. Designs test protocols and evaluation metrics, and manages technical

	queries from applicants. Reviews model architectures, test results, and compatibility with the IPT environment. Owns the design of the IPT pipeline and ensures it meets scheme requirements.
Software Developer / DevOps Engineer	Develops and maintains software for the accreditation scheme, including applicant onboarding tools and assessment systems. Supports the IPT testing application, and manages automation and integration across the scheme's infrastructure.
Legal Advisor	Provides legal oversight on scheme design and implementation. Ensures compliance with the Online Safety Act, data protection legislation, intellectual property rights, and public procurement rules.
Communications Officer	Develops and manages public-facing scheme materials (updates, timelines). Supports transparency and stakeholder communication. May coordinate responses to appeals.
Partnership Manager	Manages external partnerships and contractual arrangements. Coordinates with third-party testing bodies, dataset providers, cloud or secure infrastructure providers.

6.3.3 Project Costs

With the IPT included in the accreditation process, the estimated Project cost under the Lean Model is approximately £883,500 - £8.2 million in Year 0, with an annual average of £37,300 – £520,500 over the following years of the initial four-year testing period. The significant gaps are mostly produced by the hosting difference.

A breakdown of each project cost component is provided below.

Project	**Cost Description**	**Estimated Costs**
Launching the Scheme	This cost is associated with staff time spent on official announcement and launch of the accreditation scheme, including publishing scheme documentation, opening the application portal, and communicating key timelines and requirements to applicants.	£25 thousand - £85 thousand.

Design and Setup of the Application Platform and the IPT Testing Infrastructure	This cost involves identifying the core features of the application portal, conducting UX work to design its interface and plan the website, creating a website landing page for the screening and application submissions, hosting the portal on a live website, testing with stakeholders, and optimising user experience and functionality. Additionally, these costs are associated with establishing, either by building or procuring, a secure environment for IPT testing, including the infrastructure for hosting test datasets and conducting IPT, which involves conducting legal reviews of agreements with technical providers and stakeholders, and spending on IT services and hardware installation expenses.	£1 million - £4.5 million. The gap is primarily driven by the hosting costs' difference.
Acquisition and Preparation of Test Datasets (if IPT is included)	These costs are associated with the identification and acquisition of multiple relevant datasets, as well as selecting stratified sub-samples to prepare suitable test datasets for IPT. This involves acquiring data from providers, conducting legal reviews, establishing agreements with data partners (particularly with the providers of harmful data), transferring data from third-party providers to the hosting infrastructure, setting up data storage, and performing preprocessing tasks such as annotation, labelling, and anonymisation.	£591,568 - £2.2 million. The gap is primarily driven by the possibility that stakeholders might share the testing data for free.
Initial and ongoing training of screeners, ABA assessors, and IPT assessors	This cost is associated with providing training to those responsible for conducting the screening, the ABA, and the IPT (Ofcom internal teams or third-party assessors). It can be done internally or through an outsourced provider, like accreditation scheme experts or training services providers.	£16.7 thousand - £228 thousand. The gap is primarily driven by the difference between the in-house and outsourced delivery costs.
Conducting the IPT	These costs are associated with conducting performance testing using predefined datasets in a secure test environment, against established IPT thresholds, which involves hiring a team of software developers who are capable of delivering the IPT.	£91.2 thousand - £520 thousand (per testing round). The gap is primarily driven by demand for the scheme.

6.4 Formal Model

The Formal Model represents a full-scale, institutionalised version of the accreditation scheme. It is designed for a mature delivery environment where accreditation becomes a stable, recurring function, supported by clearly defined roles, formalised processes, and a separation between operational delivery and strategic oversight.

Unlike the Lean Model, which leverages internal flexibility, the Formal Model introduces standardised accreditation practices and dedicated governance structures. It ensures consistency, scalability, and accountability across all components of the scheme, including external assessments and testing. This model is appropriate as a **future-state configuration**, once the scheme has been piloted and refined, and demand levels justify sustained investment.

6.4.1 Model Overview

The Formal Model assumes the presence of a **dedicated delivery team** working within a structured programme governance environment. Key activities that were previously absorbed into BAU are now delivered through role specialisation. These include:

- Structured training and certification of assessors
- Dedicated oversight of ABA and IPT processes
- Formalised coordination with third-party delivery partners that is specific to the task themselves
- Standardised monitoring, evaluation, and reporting procedures

In this model, the scheme would become a sustained, professionalised programme of work, designed to meet industry best practices, support public trust, and withstand scrutiny.

A breakdown of BAU and Project activities under the Formal Model is provided below.

Formal Model	
BAU Activities	Design operating structure *(Task 1)*
	Identify technical infrastructure need *(Task 4)*
	BAU Support of application screening, ABA and/or IPT (Stage 1, 2, 5, 6, 9, 10)

	Ongoing monitoring and review of the assessors *(Stage 13)*
Project Activities	Appointment and re-appointment of parties conducting screening, ABA, and/or IPT (Task 2)
	Training and re-training of the assessors conducting screening, ABA, and/or IPT *(Task 3)*
	Obtaining testing data and the maintenance *(Task 5)*
	Build the application submission platform *(Task 6)*
	Build, borrow or buy a secure testing environment and the maintenance *(Task 6)*
	ABA Assessment Rubric *(Task 7)*
	Thresholds for IPT *(Task 9)*
	Launch the scheme *(Stage 0)*
	Delivery of application screening (Stage 3)
	Delivery of ABA *(Stage 7)*
	Delivery of IPT testing in a secure environment *(Stage 11)*
	Decision and Appeals of screening, ABA and/or IPT *(Stage 4, 8, 12)*
	End-of period scheme review and evaluation *(Task 9)*

6.4.2 BAU Costs

With the IPT included in the accreditation process, the estimated BAU cost under the Formal Model is approximately £288.1 thousand - £360.6. thousand in Year 0, £183.4 thousand - £205.7 thousand in Year 2 and 4.

We considered two levels of resourcing: a **minimum viable team** and a **full-scale team**. The timesheet of each would depend on organisational priorities and resourcing availability.

Minimum Viable Team

A breakdown of the roles of the minimum viable team is provided below.

Role	Role Description
Scheme Coordinator / Manager	Leads the day-to-day delivery of the accreditation scheme. Coordinates scheduling, documentation, applicant tracking, and delivery across all scheme stages. Manages relationships with external assessors and testing providers, ensuring delivery aligns with scheme requirements and timelines. Supports strategic oversight, planning, and risk management.
Policy & Delivery Officer	Provides operational support across the accreditation process. Manages applicant onboarding, queries, scheduling, documentation, and coordination. Reviews outputs from external assessors and testing providers for consistency with process requirements and minimum standards. Escalates issues and supports continuous improvement across scheme delivery.
Technical Lead	Provides technical input on BAU scheme needs, including identifying infrastructure requirements and advising on secure, scalable delivery options. Supports technical decision-making across the scheme.
Legal Advisor	Provides legal oversight on scheme design and implementation. Ensures compliance with the Online Safety Act, data protection legislation, intellectual property rights, and public procurement rules.

Full-Scale Team

A breakdown of the roles of the full-scale team is provided below.

Role	Role Description
Scheme Coordinator	Provides strategic leadership and overall oversight of the accreditation scheme. Owns programme governance, internal alignment, and senior stakeholder reporting. Coordinates across policy, legal, technical, and delivery functions. Ensures that all elements of the scheme, including external assessments and testing, are delivered to a high standard and in line with Ofcom's objectives.
Scheme Manager	Manages the day-to-day delivery of the scheme, including scheduling, applicant tracking, documentation, and coordination with internal teams and external delivery partners. Oversees timelines and dependencies, ensures

	process adherence, and provides operational input into planning, approvals, and risk management.
Policy & Delivery Officer	Provides hands-on support across scheme operations and delivery. Manages applicant communications, meeting scheduling, documentation workflows, and internal records. Supports onboarding, policy queries, and preparation of scheme updates. Acts as a key operational interface for applicants and suppliers.
Technical Lead	Provides technical input on BAU scheme needs, including identifying infrastructure requirements and advising on secure, scalable delivery options. Supports technical decision-making across the scheme.
Legal Advisor	Provides legal oversight on scheme design and implementation. Ensures compliance with the Online Safety Act, data protection legislation, intellectual property rights, and public procurement rules.
Partnership Manager	Manages external partnerships and contractual arrangements. Coordinates with third-party testing bodies, dataset providers, cloud or secure infrastructure providers.

6.4.3 Project Costs

With the IPT included in the accreditation process, the estimated Project cost under the Formal Model is approximately £1.4 million - £9.0 million in Year 0, with an annual average of £112,000 – £862,200 over the following years of the initial four-year testing period. These cost variations are driven primarily by differences in the hosting infrastructure.

A breakdown of each project cost component is provided below.

Project	**Cost Description**	**Estimated Costs**
Design and updates of ABA assessment rubric and IPT thresholds	This cost involves the ongoing review and potential revision of the ABA assessment rubrics as well as the thresholds for IPT.	£152 - £469.2 thousand. The gap is primarily driven by the difference between the in-house and outsourced delivery costs.

Appointment and reappointment of the assessors	This cost is associated with identifying and appointing qualified parties (whether Ofcom internal teams or third-party assessors) responsible for delivering the various stages of the accreditation process, including application screening, ABA, and IPT. This process encompasses sourcing potential candidates, defining required skills and qualifications, evaluating their competencies, and, when third-party assessors are involved, establishing formal legal agreements, along with approving and mandating their involvement.	£5.9 - £19.8 thousand
Initial and ongoing training of screeners, ABA assessors, and IPT assessors	This cost is associated with providing training to those responsible for conducting screening, the ABA, and IPT (Ofcom internal teams or third-party assessors). It is defined by the structure of the ABA and the complexity of the IPT. Additionally, it depends on the demand of the scheme and the number of applicants assigned to each assessor.	£16.7 thousand - £228.0 thousand
Acquisition and Preparation of Test Datasets	These costs are associated with the identification and acquisition of multiple relevant datasets, as well as selecting stratified sub-samples to prepare suitable test datasets for IPT. This involves acquiring data from providers, conducting legal reviews, establishing agreements with data partners, transferring data from third-party providers to the hosting infrastructure, setting up data storage, and performing preprocessing tasks such as annotation, labelling, and anonymisation.	£591.6 thousand - £2.2 million. The gap is primarily driven by the possibility that stakeholders might share the testing data for free.
Design, procurement, or enhancement of the secure IPT testing environment.	This cost involves establishing, either by building or procuring, a secure environment for IPT testing, including the infrastructure for hosting test datasets and conducting IPT. This encompasses setting up agreements with appropriate technical providers, completing necessary security checks, designing, building, and hosting the IPT assessment environment, and implementing robust security measures.	£1.0 million - £4.5 million. The gap is primarily driven by the hosting costs' difference.
Initial and periodic launches of the scheme	This cost covers the official announcement and initial launch of the accreditation scheme, including publishing scheme documentation, opening the application portal, and communicating key timelines and requirements to applicants. It also includes costs associated with any subsequent, periodic relaunches or updates of the scheme.	£25 - £85 thousand

Conducting the screening, ABA and IPT processes	These costs are associated with carrying out the application screening, the ABA, and IPT processes. This includes all activities related to inviting relevant technology providers to submit applications, reviewing submissions, conducting assessments.	£241.5 thousand - £1.1 million. The gap is primarily driven by the difference between the in-house and outsourced delivery costs.
Communicating the decisions and feedback to the applicants	This cost is associated with staff time spent communicating post-assessment approvals and rejection, with its respective feedback to applicants. It depends specifically on the demand of this accreditation scheme.	£16 thousand
End-of-period scheme review and evaluation	This cost includes conducting an end-of-period scheme review, encompassing process and impact evaluations, to assess the effectiveness of the scheme's implementation and determine whether it is achieving its objectives. It also includes reviewing and updating pricing models that detail the costs of accreditation for applicants, as well as the ABA assessment rubrics.	£35.5 thousand - £300 thousand. The gap is primarily driven by the difference between the in-house and outsourced delivery costs.

7. Constraints, Risks and Mitigations

Establishing and operating an accreditation scheme for online safety technologies involves legal, technical, commercial, and operational challenges. Some of these are fixed constraints that limit what is feasible; others are risks that may arise depending on how the scheme is designed or delivered. This section outlines the key constraints and risks, alongside potential mitigations where appropriate.

7.1 Constraints and Mitigations

Ofcom and any third-party body appointed by Ofcom will need to navigate a range of legal, technical, and operational constraints when establishing and delivering the scheme. While these limitations cannot be eliminated, careful planning, strong governance, and effective technical design can help mitigate their impact.

7.1.1 Technical Infrastructure Integration

Constraint Developing and operating infrastructure for ABA and IPT requires significant investment and integration with Ofcom's existing IT systems. Without compatibility, there is a risk of operational disruption or duplicated effort.

Mitigation Engage Ofcom's IT teams early in the design and delivery process. Use phased integration testing and ensure that infrastructure is modular and extensible to support evolving scheme requirements.

7.1.2 Security and Data Protection

Constraint Both ABA and IPT involve handling highly sensitive data, including commercial intellectual property and illegal content. Environments must comply with UK cybersecurity and legal standards, ensuring secure storage, processing, and auditability.

Mitigation Apply relevant UK Government security guidance, including the NCSC's Secure Design Principles and the Technology Code of Practice. Require formal cybersecurity audits (e.g., penetration testing), breach response protocols, and legal agreements covering data use, deletion, and confidentiality.

7.1.3 Legal Constraints on CSEA Data

Constraint Strict UK criminal law (PCA 1978, CJA 1988) limits who can access, process, and test technologies using CSEA content. While recent legislation (Online Safety Act 2023, s.214) expands the statutory defence to include individuals who are 'employed or engaged by OFCOM, or assisting OFCOM in the exercise of any of their online safety functions,' legal access remains tightly controlled, narrowing the pool of eligible testing partners and environments.

Mitigation Establish legally binding agreements with dataset holders and ensure all processing occurs within secure, UK-based environments with robust legal defence and oversight.

7.1.4 Limitations on Testing Models and Tools

Constraint Some technologies may not be easily containerised or securely deployed for testing (e.g., API-based models, cloud-native solutions). This may especially affect smaller providers or those with complex deployment architectures.

Mitigation If IPT is included, allow for flexible, secure deployment options without compromising data security or test integrity. This may require adaptable IPT infrastructure capable of supporting different testing modes, as well as procedural variation, such as adjusting how test data is accessed, to accommodate different model formats. Failure to address this constraint may result in provider exclusion (see Risk 2).

7.2 Risks and Mitigations

Beyond fixed constraints, several risks could affect the effectiveness, credibility, or uptake of the scheme. Some are internal, such as operational complexity or governance challenges, while others are external and market-driven, including misaligned incentives and reputational concerns. This section outlines key risks and how they might be managed.

7.2.1 Implementation Risks

1. Limited Safety Tech Uptake

Risk Some safety tech providers, especially smaller or emerging enterprises, may opt out due to low perceived commercial value

or limited incentive to pursue a non-mandatory accreditation.

Severity

Mitigation

Although commercial incentives are largely market-driven, Ofcom can reduce participation barriers by clearly communicating the scheme's objectives and streamlining administrative processes.

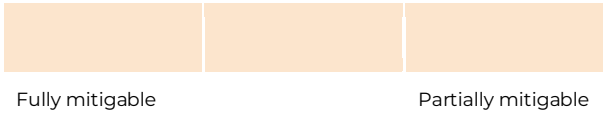
2. Exclusion Due to Technical Constraints

Risk

Providers may be unable to participate in testing due to rigid technical requirements, such as containerisation, which may not align with their system architecture or resource capacity. This risk arises if the constraint around deployment flexibility is not addressed in scheme design (see Constraint 4).

Severity

Mitigation



Offer alternative secure testing options and provide early technical guidance to help providers prepare.

3. Architectural and Dataset Misalignment

Risk

Testing environments may struggle to keep pace with evolving technologies or data types. Unrepresentative datasets could lead to misleading results, undermining trust in the scheme.

Severity

Low Medium High

Mitigation

Fully mitigable Partially mitigable Not mitigable

Segment tests by technology type, apply performance banding by deployment context, update datasets regularly, and consult external experts. These measures improve relevance but require significant technical and resourcing investment.

4. Reputational risk

Risk

If testing environments are seen as unrealistic or disconnected from real-world conditions, Ofcom may face reputational damage. Excluding an IPT stage could raise questions about the perceived robustness of the scheme, particularly among stakeholders who value independent performance validation.

Severity

Low Medium High

Mitigation

Fully mitigable Partially mitigable Not mitigable

Be transparent about the scheme's scope and limitations. Publish clear criteria, performance thresholds, and use-context guidance. If IPT is excluded, clearly explain the rationale and/or seek to incorporate key aspects of IPT into other parts of the process, for example as compatibility testing at the point of issuing a notice.

5. Incentive Misalignment and Market Distortion

Risk

Accreditation may be misused as a marketing tool, implying guarantees or endorsements Ofcom does not intend. Underperforming tools may be accredited and widely adopted, reducing trust and potentially increasing user harm.

Severity

Low Medium High

Mitigation

Fully mitigable Partially mitigable Not mitigable

While commercial dynamics are largely external, mitigations include clear communication guidelines on the meaning of accreditation and public clarification on the scope and limits of accreditation.

6. Operational Delivery Risks

Risk Ofcom faces high implementation costs, resource limitations, and potential legal challenges related to accreditation outcomes.

Severity

Low Medium High

Mitigation

Fully mitigable Partially mitigable Not mitigable

Sustained investment in staffing, governance structures, and a clear dispute resolution process can reduce these risks and support effective delivery.

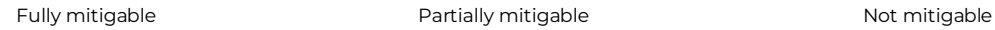
7. Governance and Oversight Risks

Risk Where third parties are used, there is a risk of limited independence or weak oversight, which could undermine the integrity of the accreditation process and result in inconsistent outcomes.

Severity

Low Medium High

Mitigation



Mitigate this risk through careful selection of third parties, clear contractual obligations, and regular audits.

7.2.2 Scalability and Sustainability Risks

As the scheme grows, operational and governance pressures are likely to intensify. If left unaddressed, these risks could reduce participation, pressure delivery capacity, or undermine public trust. Early planning, scalable infrastructure, and flexible re-accreditation models will be essential to maintain scheme performance over time.

1. Assessment Capacity

Risk Growing application volumes may overwhelm manual screening and assessment processes, slowing throughput and reducing consistency.

Severity

Mitigation

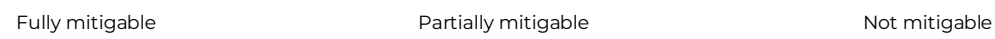
Introduce automation to support early-stage tasks (e.g. form completeness or duplicate detection) and expand assessment capacity by hiring or outsourcing more assessors where needed.

2. Infrastructure Load

Risk While core infrastructure may remain stable, increased testing volumes will raise demands on compute capacity, data throughput, and access control complexity, particularly for IPT.

Severity

Mitigation



Design infrastructure to be scalable from the beginning, taking measures like using modular architecture, adopting cloud-based or hybrid compute solutions, and planning for horizontal scaling and performance monitoring from day one. Plan for future growth by expanding compute capacity, strengthening access controls, and increasing operational support as needed.

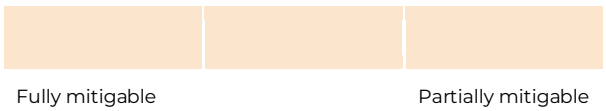
3. Re-accreditation Burden

Risk

Fixed-cycle re-accreditation may be too rigid. Frequent machine learning updates risk drifting from compliance between cycles, while overly burdensome reassessments could discourage participation, particularly from smaller providers.

Severity

Mitigation



Consider adopting a risk-based re-accreditation model, using triggers such as major updates or performance concerns. Explore the use of lighter-touch declarations for minor updates to maintain a balance between assurance and burden.

8. Appendix

8.1 Methodology

8.1.1 Approach to Evidence Gathering

To inform this report and our analysis, we adopted a mixed-methods approach that combined qualitative and quantitative evidence from three core sources:

1. Document and Literature Review:

Our evidence gathering included a desk-based review of both policy and regulatory materials as well as technical and industry literature. This informed both the process mapping and cost modelling workstreams.

Policy, Regulatory, and Accreditation Materials

We reviewed a range of official documents and grey literature to understand relevant policy frameworks, stakeholder responses, and existing accreditation models in adjacent sectors. This included:

- Ofcom consultation materials and public responses.
- Accreditation schemes in adjacent domains, including the UK Cyber Essentials scheme, medical device conformity assessments (e.g. MHRA), and the Age Check Certification Scheme.
- UK Government guidance on data security, infrastructure standards, and procurement processes, including documentation from the CPS, and NCSC.

Technical and Industry Literature

To support the design of the accreditation process and inform cost assumptions, we reviewed a broad range of technical and industry literature focused on testing infrastructure and deployment models. Key areas of focus included:

- Cloud and on-premises infrastructure costing
- GPU and compute resource planning
- Software testing environments
- API design and delivery models

Sources included technical documentation from cloud service providers (e.g. Amazon Web Services, Microsoft Azure, and Google Cloud), online safety technology providers, publicly awarded contracts for similar services, and insights from specialist infrastructure consultancies.

2. Stakeholder Engagement

We gathered practical insights from a wide range of organisations involved in technology development, accreditation delivery, and regulatory design within the online safety tech ecosystem. Engagement activities included:

Semi-structured Interviews

We conducted 22 interviews with key stakeholders, grouped into three broad categories:

- **Accreditation Users**: 11 interviews with technology providers likely to apply for accreditation, including safety tech companies and industry associations.
- **Accreditation Stakeholders**: 8 interviews with organisations likely to deliver or support accreditation activities, such as scheme operators and dataset owners from public bodies and independent or third-sector organisations
- **Adjacent Experts:** 3 interviews with international regulators, research institutions, and academics.

Follow-up Surveys

We issued detailed follow-up surveys to selected organisations within the Accreditation Stakeholder group and received 7 responses. These provided more granular data on cost and operational requirements.

External Testing

At the end of the project, we conducted 2 final validation interviews: one with a regulator overseeing a similar scheme (MHRA), and another with a senior expert from the medical sector with extensive experience in regulatory assurance. These sessions helped test key assumptions and validate the proposed cost model.

3. Market Data and Supplier Inputs for Cost Modelling

We developed a cost model informed by stakeholder input, real-world market data, and insights from our subject matter expert. Our evidence base included:

Public Procurement Data

We analysed historical UK public sector procurement datasets from projects with similar technology, assurance, and governance characteristics.

Quotes and Supplier Intelligence

- **Data acquisition:** We contacted 7 suppliers specialising in training data for large language models, specifically requesting quotes for benign and adult content datasets.
- **Infrastructure**: We gathered publicly available pricing data for on-premises infrastructure through desk research and supplier documentation.

8.1.2 Approach to Demand Modelling

As noted earlier, the demand modelling is based on two mathematical models:

1. **Estimation of the initial demand**: This model identifies the initial pool of potential applicants that meet the scheme's eligibility requirements (as previously outlined) and estimates the proportion likely to participate in the accreditation process.
2. **Estimation of the demand during the subsequent periods:** This model projects potential future demand by accounting for reapplications from previously unsuccessful applicants and new entrants who may be willing to apply in subsequent cycles.

Demand Estimation for Year 0

The initial demand is estimated through the following steps:

- **Step 1: Estimate the pool of possible applicants:**
    - **Calculation 1:** Total number of global safety tech providers × Percentage of providers aligned with relevant safety tech taxonomies × Percentage of providers that are SMEs or large companies × Percentage of companies specifically dedicated to addressing CSEA or terrorist content
- **Step 2: Estimate the companies that are willing to apply.**
    - **Calculation 2:** Calculation 1 × Willingness to apply

Demand Estimation for Year 2 and Thereafter

From year 2 onwards, the ongoing demand is estimated as it follows:

- **Step 1: Estimate the rejected providers from the previous accreditation process.**
    - **Calculation 1:** Number of providers in the previous period × (1 - Success rate)
- **Step 2: Estimate the number of new providers based on the growth rate over 2 years.**
    - **Calculation 2:** Number of providers in the previous period × (((1 + Growth rate of global providers)^2) - 1)
- **Step 3: Multiply the pool of possible applicants (including newcomers and previously rejected applicants) to the willingness to apply rate.**
    - **Calculation 3:** (Calculation 1 × Willingness to apply) + (Calculation 2 × Willingness to apply)

Model Variables

The following variables inform the demand estimation calculations:

- **Total number of global safety tech providers:** Estimated total number of safety technology companies operating worldwide.

- **Percentage of global providers based in the UK:** Proportion of global safety tech companies with their primary base in the United Kingdom.
- **Percentage of UK-based providers aligned with relevant safety tech taxonomies:** Share of UK-based providers whose technologies fall into the defined categories (e.g., system-wide governance, platform-level safety, user-level protections, or network filtering).
- **Percentage of providers that are SMEs or large companies:** Proportion of eligible companies that are small and medium-sized enterprises or large corporations, typically excluding micro-businesses or sole traders.
- **Percentage of companies specifically dedicated to addressing CSEA or terrorist content:** For the purposes of this estimation, this represents the proportion of companies whose core focus is to combat CSEA or terrorist content.
- **Willingness to apply:** Estimated percentage of eligible providers expected to apply for accreditation (from Year 0 onwards).
- **Number of providers in the previous period:** Total number of providers who applied in the immediately preceding year, used for calculating demand in subsequent periods.
- **Success rate:** Estimated percentage of applicants expected to meet certification requirements and receive accreditation.
- **Growth rate of global providers:** Projected annual growth rate in the total number of safety tech providers globally.
- **Re-application rate:** Estimated percentage of previously unsuccessful applicants expected to reapply in later cycles (from Year 2 onwards).

Taxonomy Classification of the UK Safety Tech Sector According to 'The UK Safety Tech Sector: 2024 Analysis' report[33]

Safety technology taxonomy that are within the scope of this Tech Accreditation scheme includes:

- **System-Wide Governance:** Automated identification and removal of illegal content: Use of technology to detect and facilitate the removal of illegal CSEA material and terrorist content, including imagery and video.
- **Platform-level**: Support for content moderation by identifying and flagging potentially illegal content or conduct, such as grooming, hate crime, harassment, or suicide ideation. This also includes harmful content or conduct that breaches site terms and conditions (e.g. cyberbullying, extremism, advocacy of self-harm), detection of and response to fraudulent activity, and tools that reduce moderators' exposure to harmful content.
- **Age-oriented online safety**: Focuses on enabling age-appropriate online experiences through age assurance and verification services that limit children's exposure to harmful content, or through the creation of child-safe content.

[33] DSIT, The UK Safety Tech Sector: 2024 Analysis, 2024

Safety technology taxonomy that are outside the scope of this Tech Accreditation scheme includes:

- **User protection**: User-, parental-, or device-based tools that can be installed on devices to help protect individuals from online harm.
- **Network filtering**: Products or services that actively restrict access to harmful content by blacklisting or blocking it. Often used in schools, businesses, or homes to safeguard users.
- **Information environment**: Detection and flagging of false, misleading, and/or harmful narratives through fact-checking and disruption of disinformation (e.g., provision of trusted sources).
- **Online safety professional services**: Advisory support for implementing technical solutions, developing safer online communities, and embedding safety-by-design principles.

8.1.3 Approach to Cost Modelling

The cost modelling approach is based on two primary cost types: **BAU costs** and **project costs**. Both are analysed across a range of scenarios to provide a comprehensive view of potential financial requirements.

Cost Calculation Methodology

Costs are estimated using an evidence-based **price-quantity product**. In particular, the quantity is determined by the number of units required and the frequency with which they are needed.

BAU Costs

Prices are based on Ofcom-published **salary data for specific roles**, while quantities are calculated by multiplying the **number of staff** assigned to each task by the **number of days required to complete it**. Task-specific time estimates were developed by the PUBLIC team, drawing on research findings.

Project Costs

Estimated prices reflect the **cost of the products or services** purchased, while quantities are determined by the **amount needed per use** and the **frequency of use**. The delivery model introduces an important distinction that has to be taken into account:

- **In-house:** For in-house versions of these costs, costs are calculated based on the number of personnel required and their associated salaries.
- **Outsourced:** For outsourced versions, costs are based on unit prices and frequencies, multiplied by pricing estimates informed by market research.

Each of these costs has a **minimum and a maximum value**, generating two new possible cost scenarios, these are then averaged to produce a mid-range estimate for comparative purposes.

Limitations

From a cost estimation perspective, two key limitations emerged:

A. Undefined Crucial Cost Determinants

Accurately estimating the **cost of the ABA** requires clarity on the number of questions and supporting documents involved.

A similar challenge applies to the **IPT**, where several cost-driving variables, such as dataset acquisition or the potential need for an on-premise data centre, will only be determined at a later stage.

B. Lack of Comparable Accreditation Process

A key limitation in this costing exercise is the absence of a directly comparable accreditation process for benchmarking purposes. A key assumption in the cost estimation was that the IPT process could be cautiously compared to the ACCS accreditation scheme, given its similarly high technical standards. This assumption was necessary due to the lack of directly comparable IPT processes identified in other organisations.

To mitigate this constraint, the modelling adjusted several assumptions and expanded the range of scenarios to capture plausible cost variability.

C. Significant Variables Cannot Be Benchmarked

The acquisition of testing datasets is one of the largest projected costs in the model. However, due to legal restrictions surrounding CSEA content, commercial procurement is not a viable option. As a result, the analysis relied on assumptions about the cost of obtaining legal data. This may introduce an overestimation bias, since such datasets are most likely to be sourced from certified philanthropic institutions and governmental bodies that are legally authorised to handle this type of content and would likely provide access at a lower cost to Ofcom.