

Ofcom Tech Accreditation Landscape

Final deliverable

June 2023



Table of Contents

Sections

Reference

Executive Summary

An overview of the key research findings

Page 03

Research Context

Context of the project, objectives and its relevance

Pages 04-06

Methodology

Research methodology and limitations

Pages 07-10

Key Takeaways

Our project findings, key takeaways and high-level considerations for Ofcom related to the landscape of accreditation approaches

Pages 11-19

Further Insights

- **Longlist of Approaches Library**
The list of accreditation approaches reviewed during the research and an advantage / disadvantage analysis for each approach
- **Deep Dive Case Studies**
The 3 selected case study deep dives with an in-depth overview of the selected approaches and the key implementation considerations

Pages 20-64

Pages 65-93

Conclusion

Conclusion

Pages 94-96

Appendix

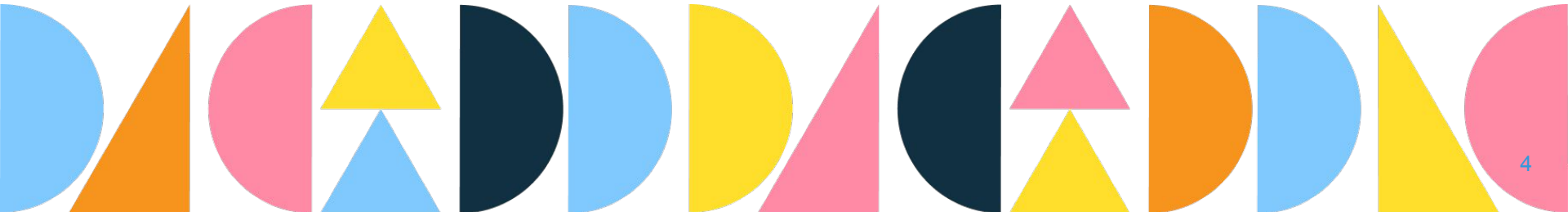
- **Project Definitions**
- **Reader's guide for longlist approaches library and accreditation process**
- **Bibliography**

Pages 97-105

Executive Summary

- In May 2023, Ofcom commissioned PUBLIC to **help develop their knowledge and evidence base on how products and services are currently being evaluated and accredited in different sectors**. This 7-week project aimed to inform Ofcom's development of a robust and effective accreditation process. This report includes our findings from the research project.
- Our research has focused on "Accreditation Approaches" as typically referred to:
 1. An assessment of the **conformity of products/services or providers of products/services with a set of criteria**
 2. An assessment of the **competence and impartiality of an organisation/individual that performs those activities**
- PUBLIC followed a two-phase approach to the research. During Phase 1, the team gathered **evidence on 11 accreditation approaches across 5 industries**. During Phase 2, the team conducted a **priority scoring** exercise and then **develop in-depth case studies for Ofcom's highest priority approaches**. The research methodology centred on desk research, with the team reviewing **over 70 sources** to inform the analysis.
- Our research has highlighted **six pillars of a robust and effective accreditation process for innovative technologies for Ofcom to take into consideration when shaping it's approach to accreditation of technologies**:
 1. Where possible, prioritise **principles over prescriptive rules** to allow flexibility
 2. Ensure **adaptability to changing circumstances**
 3. Enable **uptake through a scalable process**
 4. **Reduce burden for applicants** to incentivise uptake
 5. **Identify required expertise and skills** early
 6. Establish **strong governance practices** upfront
- PUBLIC have uncovered **3 high-value areas of further research**. These are: 1) accreditation process design & roadmapping, 2) Ofcom capability mapping and 3) in-scope technology landscaping.
- As a quick-turn research project, this work has allowed the project team to **build an initial understanding of the landscape of accreditation approaches, with further work to be done to validate these findings and apply to Ofcom's context**.

Research Context



PUBLIC is supporting Ofcom in understanding how accreditation processes are developed, evaluated, and operationalised in practice

1

Ofcom has the **power under section 121 of the Online Safety Act to require certain regulated services to use accredited technology.**

Technology will be considered as 'accredited' **where it is has been accredited by Ofcom (or a person approved by Ofcom) as meeting minimum standards of accuracy** in the detection of CSEA and/or terrorism content (as the case may be).

2

In this context, Ofcom is seeking to **develop its knowledge and evidence base on how technologies are evaluated and accredited.**

This research project aims to **inform Ofcom's development of a robust and effective accreditation process.**

3

The way in which accreditation approaches are developed, evaluated and operationalised in practice **varies depending on the sector, type of accreditation, regulatory approach and stakeholders involved.** In such a diverse landscape, PUBLIC's focus has been on **identifying common practical challenges and opportunities** for the accreditation approaches in scope.

Despite a robust approach, Ofcom should bear in mind the following limitations when analysing our findings

Short project timeframes

Due to a tight 7-week project timeline, **we have focused our review of the most relevant and valuable issues on each approach and prioritise clearly** to avoid over-scoping the research.

This has limited our capacity to explore a greater number of accreditation approaches and dive deeper into additional case studies.

Stakeholder engagement

We have relied on desk research to provide Ofcom with an overview of existing approaches to evaluation and accreditation of products and services.

Limited engagement with accreditation stakeholders have limited our ability to cover research gaps (for more detail on research gaps please refer to slide 94).

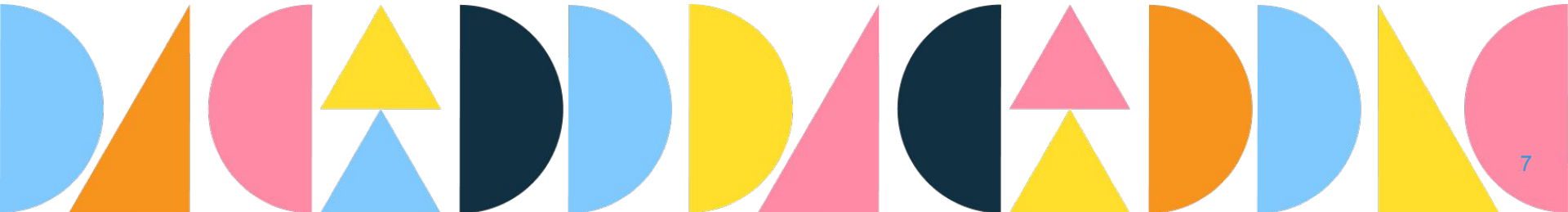
Scope of Accreditation Approaches

Based on Ofcom's steer, when conducting desk research we prioritised **diversity and breadth of approaches outside of online safety** and accreditation approaches for **both technology and non-technology** related products and services (e.g., sustainability).

Some of our findings related to those sectors and services might not be directly comparable with accreditation of technologies.

PUBLIC and Ofcom have aligned on research scope and limitations at kick-off and throughout project delivery

Methodology



Our methodology is built on pre-identified concepts and processes from PUBLIC's technology accreditation expertise

Types of Approaches in Scope

Based on parties involved	Third-Party Accreditation	- This type of accreditation is carried out by an approved third-party organisation assessing technology, product or service against certain requirements via testing, auditing and certification, etc. - Third-party conducting assessment is typically appointed by regulators and qualified in line with relevant standards (i.e. ISO/IEC 17065).
	Mixed Approach	- Mix approach combines multiple accreditation approaches (e.g. verified self-assessment in combination with formal third-party accreditation, self-assessment overseen by a third party). - This type of approach may or may not involve a third-party body serving as a formally approved accreditation body, an informal assessment body, or an oversight body, etc.
Based on regulatory approach	Rules	Approach where the primary focus is on compliance with a set of rules (i.e technical standards) in a prescriptive way.
	Principles	Approach where the primary focus is on adherence with underlying principles that describe the objective of the accreditation scheme.

Types of Accreditation Subjects in Scope

Specific Service

Accreditation schemes available for **organisations that perform specific services** related to a particular industry (either voluntary or mandated by law/regulation).

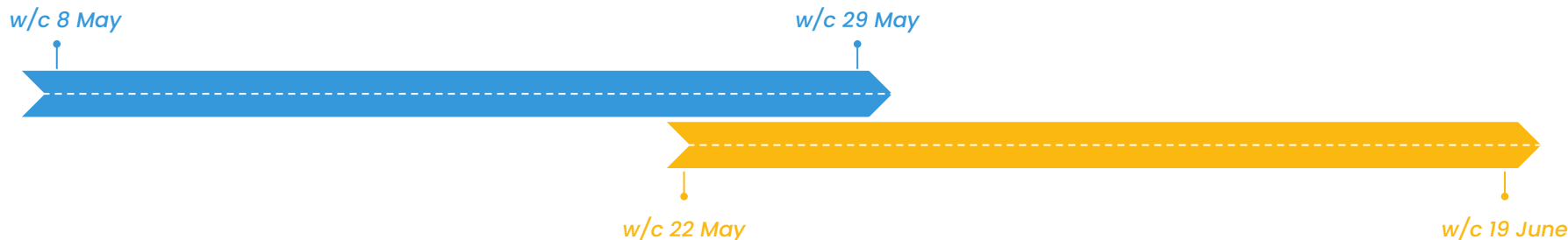
Product

A product (technology and non-technology related) is accredited or assessed against a set of criteria to ensure it meets specific criteria usually related to safety, quality, and usability.

General

Any organisation can undergo accreditation regardless of the product or service they are developing.

This project spanned 7 weeks over two phases to develop a landscape review of technology accreditation approaches



Phase 1: Landscape Mapping

Key Activities

- Desk research
- Development of longlist approaches and criteria
- Advantage and disadvantage analysis

Deliverables

- **Longlist approaches library**
- **End of Phase 1 deliverable**



Phase 2: Deep Dive

Key Activities

- Prioritisation framework
- Downselect case approaches for case studies
- Case study deep dive analysis

Deliverables

- **Prioritisation framework**
- **Case study deep dive**
- **Final report**
- **Presentation**

We reviewed more than 70 sources and built a long list of 11 accreditation approaches from 5 different sectors

Longlisted Accreditation Approaches*

	Medical Laboratory Accreditation
	Certification Body Accreditation
	Independent Audit of AI Systems
	Cyber Assessment Framework
	TEMPEST and EMS Accreditation
	B Corp Certification
	LEED Certificate
	EASA Part 145 Accreditation
	Digital Technology Assessment Criteria
	Singapore's approach to AI Governance
	Cyber Essentials/Cyber Essentials Plus

Key Considerations

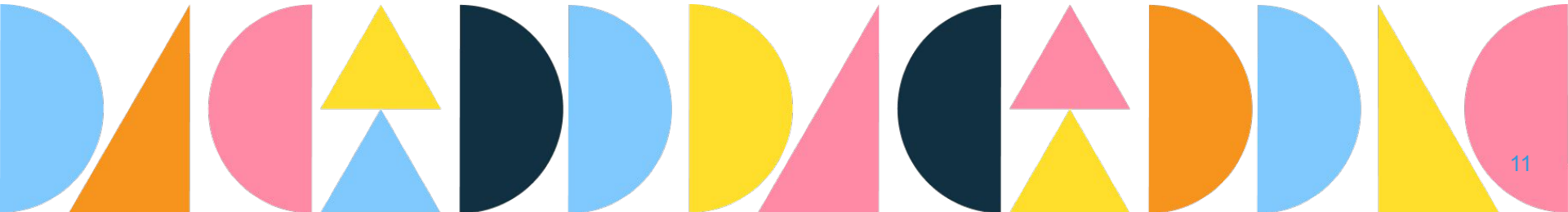
- **Variety of Sectors and Approaches.** The chosen accreditation approaches combine a variety of sectors, types of approach, subjects being accredited and processes.
- **Value to Ofcom.** We pre-identified and agreed with the Ofcom team the relevant criteria we wanted to identify for each accreditation approach:
 - Type of approach
 - Subject
 - Process
 - Standards
 - Legislation
 - Assessment criteria
- **Evidence-based knowledge.** We developed the longlist of approaches depending on how much evidence and public information was available to ensure we gathered a sufficient evidence base.

KEY

Health	
AI	
Cyber	
Sustainability	
Aviation	

Note: This research aims to build evidence base of technology accreditations for Ofcom. Given Ofcom's existing knowledge and engagement with the ICO on age assurance, accreditation approaches to age assurance were not prioritised in this project.

Key Takeaways



Following a literature review of 70+ sources, we selected 11 accreditation schemes to analyse

Type	Sector	Scheme	Accreditation Body	Standards Body	Subject	
Third-party Accreditation		Medical Laboratory Accreditation	UKAS	ISO	Medical Laboratories	
		Certification Body Accreditation	UKAS	ISO	Certification Bodies	
		Independent Audit of AI Systems	ForHumanity	ForHumanity	Any organisation	
		Cyber Assessment Framework	NCSC	IEC, ISO, NCSC	CNI's, Gov Bodies	
		TEMPEST and EMS Accreditation	NCSC, Test Lab	NCSC	ICT Infrastructure	
		B Corp Certification	BLab Country Ch.	BLab Global	Any organisation	
		LEED Certificate	USGBC; GBCI	USGBC	Buildings	
		EASA Part 145 Accreditation	EASA	EASA	Aviation maintenance organisations	
Prioritised for deep-dive	Mixed Approach		Digital Technology Assessment Criteria	NHS England	NHS England, ISO, ICO, NCSC	Health technologies
			Singapore's approach to AI Governance	PDPC, IMDA	PDPC, IMDA	AI Systems
			Cyber Essentials/Cyber Essentials Plus	IASME	NCSC	Any organisation

We used a prioritisation matrix based on six criteria to downselect three case studies for a deep-dive to understand the accreditation process in detail. Please see separate prioritisation matrix deliverable for more on the prioritisation.

Our three shortlisted deep dive case studies all share mixed approach characteristics using different assessment methods

Prioritised for deep-dive

Mixed Approach

Type	Sector	Scheme	Notes
		Digital Technology Assessment Criteria	Self-assessment is conducted of their health technology against the DTAC questionnaire. To procure such technology, a NHS local healthcare provider will conduct an independent assessment to ensure that the technology meets DTAC criteria.
		Singapore's approach to AI Governance	Self assessment is verified by application completion using a AI Verify automated assessment tool. AI Verify is developed by third parties (i.e. IMDA and PDPC) and the assessment is conducted automatically with oversight from IMDA and PDPC.
		Cyber Essentials/Cyber Essentials Plus	CE requires self accreditation verified by the internal board of an organisation and approved by an IASME assessor. CE+ requires both self accreditation and third party accreditation via technical auditing and on-site assessment conducted by a licensed third party certification body.

We have summarised key research findings and considerations for Ofcom by sector, process stage, and approach type

PUBLIC

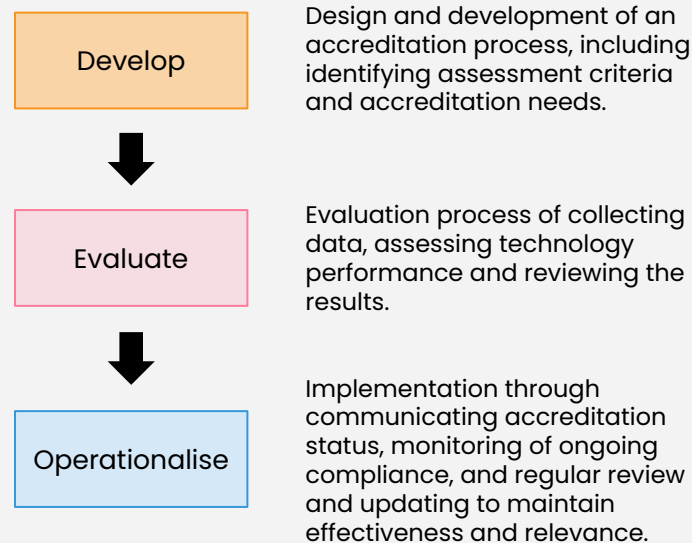
Accreditation Approach

We analysed 11 accreditation schemes across 2 types and 5 sectors.

Type	Sector	Scheme
Third-party Accreditation		Medical Laboratory Accreditation
		Certification Body Accreditation
		Independent Audit of AI Systems
		Cyber Assessment Framework
		TEMPEST and EMS Accreditation
		B Corp Certification
		LEED Certificate
Mixed Approach		EASA Part 145 Accreditation
		Digital Technology Assessment Criteria
		Singapore's approach to AI Governance
		Cyber Essentials/Cyber Essentials Plus

Accreditation Process Stage

For each scheme, we researched how it has been developed, evaluated and operationalised.



PUBLIC's analysis has highlighted six pillars of a robust and effective accreditation process for technologies

PUBLIC



Prioritise principles over rules to allow flexibility

- Where possible, prioritise **principles-based approaches** to allow for **more flexibility, adaptability** to change and **streamlined governance focused on continuous improvement** of the organisation's processes.
- For this reason, principle-based accreditation is **particularly popular in emerging tech sectors** (i.e. AI, Cyber and Healthtech)



Establish strong governance practices upfront

- **Community engagement** has been best practice in multiple sectors (i.e. Cyber and Sustainability) to **enhance the feedback loop** throughout the development, implementation and maintenance of accreditation.
- Establishing **clear KPIs for monitoring & evaluation of accreditation schemes** helps track the impact of accreditation and **inform maintenance**.



Ensure adaptability to changing circumstances

- **Regular review** of the accreditation scheme, **based on assessor and applicant feedback**, helps refresh requirements to address **evolving challenges**.
- **Periodic renewal** – often on an annual basis – ensures **ongoing adoption monitoring** and provides **reassurance** to organisations and the public.



Ensuring a scalable process

- **A multi-tiered, mixed-method accreditation** allows organisations to choose the best-fit scheme based on size, revenue and organisational needs **avoiding the 'one-size-fits-all' approach**.
- In certain circumstances, **automated assessment tools** can facilitate cost-effective and scalable accreditation. (See case study 2)



Identify required expertise and resources early

- **The upfront design and development** of an accreditation scheme (incl. process design, and software development) and **technical inspections/auditing** entail most costs and expertise/resource requirements.
- **The number of involved parties varies** for different accreditation. **Early engagement** is crucial to align priority and source expertise.



Reduce friction for applicants to incentivise uptake

- **Transparent** processes and criteria, and **clear questionnaires** increase uptake.
- **Pricing and timeline** of accreditation needs to reflect **organisation's size, accredited subject, and complexity** of the assessment.
- **Tools and learning resources** sufficiently prepare applicants for accreditation and thus increase the success rate.

Accreditation schemes vary on each sector to best align with the market trends and regulatory needs (1/2)

PUBLIC

Key Findings



Health

- Historical and **tested approach** (via UKAS) to medical laboratories, imaging diagnostics and physiological services and laboratories, but **novel approaches** (i.e. DTAC) are arising for innovative **HealthTech**.
- Due to the Covid-19 pandemic, UKAS had to **adapt and test new assessment approaches** to support government requirements, proving the adaptability of their approach.



AI

- Constantly evolving market has caused **duplicative efforts**, and **long-term “draft” principles**. Long-term review periods **delay deployment** of schemes, only to be quickly put back on review to address **changes in fast moving markets**
- The **trialing of automation tools** allows for easy **scalability** and **flexibility**. Automation tools (i.e. Singapore's) also support **independent learning of compliance**.



Cyber

- **Principle-based approaches are widely adopted in cyber** to allow for scalability and adaptability. **Layering technical standards** embeds robustness to appropriately assess technical products and systems.
- Given the typical **technical complexity** in cyber, **significant resource and highly skilled personnel** are required to appropriately deliver the schemes and ensure compliance.

Key considerations for Ofcom

- **Mature approaches are not always well suited for accreditation of novel technologies**, even within the same industry. **Accreditation of rapidly evolving technologies requires high flexibility with limited resources**.
- **Identify and acquire capabilities required upfront, test pilots and engage with relevant industry stakeholders**, to ensure accreditation adapts quickly to changing circumstances.
- Evolve with the market by **evaluating and adapting as the market evolves**. It is worth noting long timeline of accreditation design process may stagnate the momentum and cause duplicative efforts.
- **Automation tools** may help with scaling and adapting quickly, but need **trialing** for accuracy and efficacy. Additionally, **a large upfront burden** is taken in setting up and building the automation tool.
- **Layering non-technical principles with technical standards** can promote comprehensive assessment for organisations.
- The more technical the accreditation process is, the more technical staff and standards are needed **causing increase in time and funding** for set-up, delivery, and management.

Accreditation schemes vary on each sector to best align with the market trends and regulatory needs (2/2)

PUBLIC

Key Findings

- Variety of **mixed based review methods** from points system to tiered accreditation allows to **tailor the approach** to sub sector and market needs.
- **Community driven approaches** (i.e. early engagement with providers, training workshops, networking events, newsletters, directories, annual conferences, etc.) encourage **lifelong adherence** to standards and **strong accreditor-applicant relationships**.



Sustainability



Aviation

- **Highly regulated** space encourages **harmonisation** across accreditation processes when the use of accreditation is intended to be adopted in several jurisdictions.
- **Regional dependency** given regulation ownership and implementation relies on **highly skilled personnel and technical expertise**.

Key considerations for Ofcom

- **Tiered or points based approaches** allow for SMEs to apply for certification levels appropriate for their **business maturity**, but also poses **risk** that the lowest certification level comparatively is **inadequate**. **Transparency around metrics and the assessment process** are key to mitigate this risk, including companies themselves producing **annual impact/transparency reports**.
- Fostering a **community** around the accreditation scheme will support the accreditation team to **stay up to date on trends** and applicants to **commit long term to standards/principles**. It will encourage bodies to **re-apply for certification** and **ease data collection** for evaluation and market analysis.
- If taking a global approach to accreditation, it is essential to implement **harmonisation processes, identify counterparts and agencies in other jurisdictions and develop maintenance schemes** to make sure any change to the process or standard is replicated across all jurisdictions.
- **In-house regional expertise** is best practice to build, manage, and adapt regional specific accreditation process.

Throughout each stage of the accreditation process, we found widely adopted practices that enhance its effectiveness

PUBLIC

Accreditation Process Stages

	Key Findings	Key considerations for Ofcom
Develop	- Assessment criteria are often rooted in existing legislation, regulations and international principles and aligned with industry best practices, which bring them together into single, streamlined accreditation. Engagement with standards/accreditation bodies in agencies and technology compliance community helps identify user needs, bring in external expertise, and ensure relevance and acceptance.	Identify and consolidate relevant standards, principles and assessment criteria to ensure consistent enforcement of regulatory requirements. Consider a feedback loop (i.e. consultation, working group) with the ecosystem to benefit from external expertise, best practices and industry feedback.
Evaluate	- Additional technical testing is often needed for a high level of assurance, incurring higher costs and a longer timeline, due to the requirements for testing datasets, technical environment, experts/engineers and qualified assessors. - Providing post-assessment feedback to the applicants can help with remediation if failed initially, and drive continuous improvement in practices and compliance.	- Conduct further research on potential technical testing methods and resources/expertise required to develop appropriate testing infrastructure - Consider multi-layered approaches including non-technical assessment to provide flexibility and reduce burden. Embed remediation and post-assessment feedback to the accreditation process.
Operationalise	- Most accreditation schemes require periodic renewal to ensure ongoing compliance, including annual assessment, reporting, and re-accreditation/certification. Regularly review and update of an accreditation scheme keeps it up to date with evolving technology development and addresses identified shortcomings.	Consider the requirements of periodic renewal. Renewal frequency and format needs to balance the needs for ongoing adoption in response to evolving circumstances and the burden of re-assessment. Establish a plan for regular review upfront including baseline review and ongoing impact evaluation.

The type of accreditation approach influences adoption, effort, burden on parties and adaptability of the process

Key Findings

Key considerations for Ofcom

Accreditation Approaches

Third-Party

- **Third party accreditations tend to rely on rules-based approaches to accreditation.** They are more focused on compliance against a specific set of **standards (i.e ISO standards)**.
- There is **heavy reliance on auditing processes conducted by third-party entities** (i.e UKAS) to confirm compliance with standards.
- **High level of assurance and confidence** in accreditation results due to rigorous, non-flexible processes.

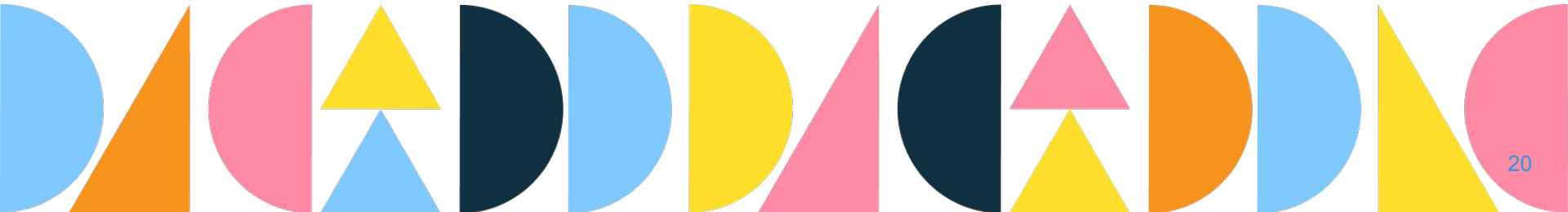
- Third party accreditation approaches are more focused on compliance with a set of rules and standards rather than **improvement of management and performance**.
- Utilising a **third party auditing entity with experience on accreditation schemes could facilitate implementation**
- Third-party accreditation approaches **are less adaptable to dynamic markets and sectors** due to the number of parties and specific rules in place.

Mixed

- Mixed approaches are usually **more focused on qualitative improvements and frameworks rather than standards**.
- Mixed approaches are applicable to **wide range of industries and products and services due to their flexibility and adaptability**.
- **They remain still well suited for a third-party auditor to ensure compliance** with the process and standards set by accreditation body.

- **Mixed approaches reduce the burden/expertise/effort both for accreditation bodies and for candidates** as the assessment is shared between both parties.
- Ofcom might consider introducing a mixed approach to **accreditation of technologies to facilitate flexibility, scalability and incentive compliance**
- Providing entities with the opportunity to conduct self-assessments could **incentivise adoption across the supply chain and facilitates compliance in case of an independent audit**.

Further Insights: Longlist of Approaches Library



Third-Party Accreditation

Medical Laboratory Accreditation

Medical Laboratory Accreditation

Approach type: Third-party accreditation

Approach Summary

An assessment carried out by UKAS accreditation to ensure **testing services in medical laboratories meet the relevant requirements related to integrity, impartiality and competence**, and the ability to demonstrate that specific testing activities performed in the laboratory are performed within the criteria set out in the specific ISO/IEC 17025 criteria.

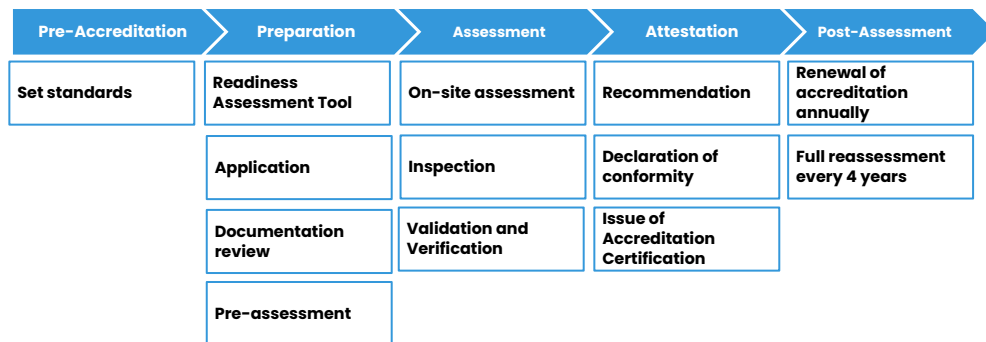
Sector	Geography	Accreditation Body	Standards Body
			

Necessity: Voluntary

Standards: [ISO/IEC 17025](#)

Source(s): [Medical Laboratory Accreditation - ISO 15189](#)

Process overview



Key Assessment Criteria

Technical/Non-Technical. On application the following information is requested:

1. Medical laboratory fields
2. Products and materials that are tested
3. Types of examination/technical fields/activities
4. Equipment used
5. Measurement principle and main SOP reference
6. Laboratory location

Both the responsibilities among and within each entity are clearly set out during the process

PUBLIC

Pre-Accreditation

Preparation

Assessment

Attestation

Post-Assessment

Standards Body

ISO/IEC 17025 standards are set and published.



Accreditation Body



Reviews application and assesses service against ISO/IEC 17025 **minimum standards**.

Conducts the assessment, which includes visiting the premises. Depending on the organisation size, the process could take between **6-12 months** until accreditation.

UKAS Assessment Manager submits their recommendation to an **independent decision-maker** within UKAS.

Accreditation is confirmed on an **annual basis** through surveillance activities, **with a full reassessment every fourth year**.

Medical Laboratory



Conducts a **readiness assessment evaluation** against the standards and submits an application to UKAS.

Provides suitable evidence to UKAS Assessment Manager that they have addressed any observations.

Following ratification of the decision to grant accreditation, the organisation will be **notified in writing with a certificate of accreditation**.

Go through accreditation confirmation on an **annual basis** and a **full reassessment every fourth year**.

This approach is tailored to the nature of the activities performed PUBLIC by medical laboratories, requiring rigorous on-site auditing

Advantages	Disadvantages
 Costs vary depending on the size and type of organisation, activity and type of accreditation which means organisations will pay in proportion to the size and complexity of their operations.  UKAS offers both pre-assessment and training support for organisations who want to go through the accreditation process. This will facilitate familiarity with the process and timelines.  Any changes in regulation, standards or industry practice can be easily adopted to this approach due to the expertise and scale of UKAS. Most changes will have to be properly communicated and aligned with UKAS.	 The full accreditation process might take between 6 to 12 months (even more depending on the size of the organisation looking to be accredited).  UKAS needs to staff an Assessment Manager who will own the process of accreditation and a team of people with relevant expertise conducting on-site visits.  There is limited information available about the type of assessment criteria (technical and non-technical) that organisations will be evaluated against after submission of the application.  Due to the nature of operations that medical laboratories perform (testing, calibration, measurement) this process can only be replicated to similar activities within other industries, which limits its scalability.  UK regulation specific and dependent and therefore there may be contextual and legislative nuances specific to this approach.

Third-Party Accreditation

Certification Body Accreditation

Certification Body Accreditation

Approach type: Third-party accreditation

Approach Summary

An assessment to demonstrate that **certification bodies in the health sector are technically competent to audit and certify activities** in accordance with the requirements of national and international standards and regulations. Certification bodies are independent, impartial bodies that operate one or more certification schemes to certify clinical services.

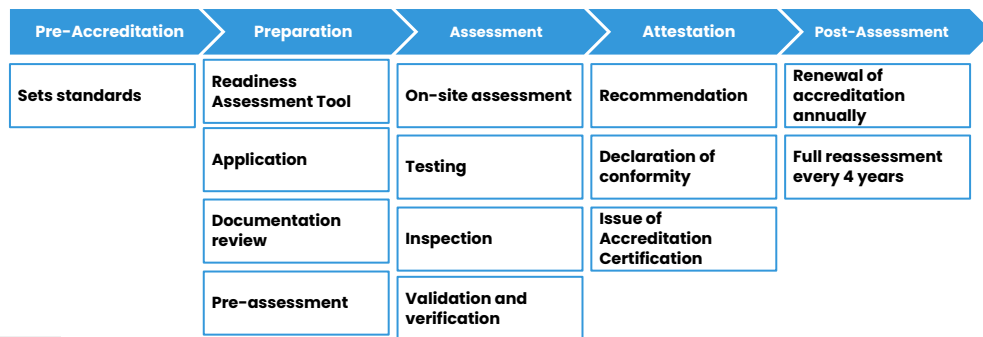
Sector	Geography	Accreditation Body	Standards Body
			

Necessity: Voluntary

Standards: [ISO/IEC 17065:2012](#)

Source(s): [Certification Body Accreditation](#)

Process overview



Key Assessment Criteria

Technical/Non-Technical. On application the following information is requested:

1. Location and type of activities to be performed
2. Management Systems

Although the activity being accredited is only applicable to certification bodies, the process follows UKAS' standard approach

PUBLIC



Standards Body



ISO/IEC 17065:2012 standards are set and published.

Accreditation Body



Reviews application and assesses service against ISO/IEC 17065:2012 **minimum standards** in a specific deployment context.

Conducts the assessment, which includes visiting the premises. Depending on the organisation size, the process could take between **6-12 months** until accreditation.

Assessment Manager submits their recommendation to an **independent decision-maker** within UKAS.

Accreditation is confirmed on an **annual basis** through surveillance activities, **with a full reassessment every fourth year.**

Certification Body in Health sector



Conducts a **readiness assessment** against the standards and submits an application to UKAS.

In case of observations, organisations will have **approximately 12 weeks to provide suitable evidence** to Assessment Manager that they have been addressed.

Notified in writing with a certificate of accreditation.

Go through accreditation confirmation on an **annual basis** and a **full reassessment every fourth year.**

Approach used to “check the checkers”: accreditation certification bodies who will assess compliance with standards

PUBLIC

Advantages	Disadvantages
 Costs vary depending on the size and type of organisation, activity and type of accreditation which means organisations will pay in proportion to the size and complexity of their operations.  This is a standard approach to the accreditation of entities that will provide certifications, meaning that the approach is giving transparency to organisations that the ‘checkers have been checked’.  UKAS offers both pre-assessment and training support for organisations who want to go through the accreditation process. This will facilitate familiarity with the process and timelines.  Any changes in regulation, standards or industry practice can be easily adopted to this approach due to the expertise and scale of UKAS. Most changes will have to be properly communicated and aligned with UKAS.	 The full accreditation process might take between 6 to 12 months (even more depending on the size of the organisation looking to be accredited).  UKAS needs to staff an Assessment Manager who will own the process of accreditation and a team of people with relevant expertise conducting on-site visits.  There is limited information available about the type of assessment criteria (technical and non-technical) that organisations will be evaluated against after submission of the application.  UK regulation specific and dependent and therefore there may be contextual and legislative nuances specific to this approach.

Third-Party Accreditation

Independent Audit of AI Systems (IAAIS)

Independent Audit of AI Systems (IAAIS)

Approach type: Third-party accreditation

Approach Summary

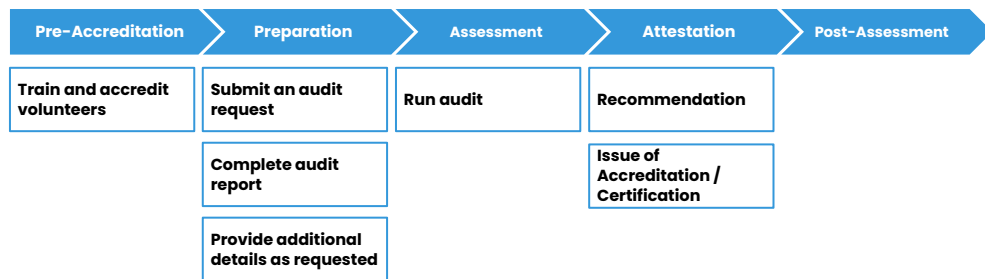
A risk-based approach for **building trustworthy AI across the following areas: Ethics, Bias, Privacy, Trust, and Cybersecurity**. The process is built and driven by **accredited volunteers registered and trained by ForHumanity**. Interested companies can submit audit reports and additionally requested data for assessment.

Sector	Geography	Accreditation Body	Standards Body
			

Necessity: Voluntary

Standards: ForHumanity's AI and automated systems 'Trust Principles'

Process overview



Key Assessment Criteria

Technical/Non-Technical. The 8 standards or "Trust Principles" (Predictability, Transparency, Understanding Control, Security, Fairness, Equity and Morality) are assessed against each party involved in a typical financial audit: auditor, compliant entity, society, and the five Audit Rules:

1. Binary- compliant/noncompliant
2. Measurable, unambiguous
3. Iterated and Open-sourced
4. Consensus-Driven
5. Implementable

The process relies heavily on training of volunteers by ForHumanity, developed through crowd-sourcing and collaboration

PUBLIC

Pre-Accreditation

Preparation

Assessment

Attestation

Post-Assessment

Standards Body



Drafts Trust Principles and **consult with experts and trained volunteers.**

Accreditation Body



Trains accreditate volunteers to be **official 'IAAIS Auditors'.**

Appoints a trained accredited AI Auditor. Communicates with applicant requirements.

Runs audit on AI systems and organisation.

Provides results with recommendations for improvement. If successful, **issues certificate** to applicant.

Organisation



Submits an **audit request** to ForHumanity. **Completes an audit report** and provides other requested material.

ForHumanity's IAAIS is a risk-based approach delivered by a volunteer accreditation body, currently under review and revision

PUBLIC

Advantages	Disadvantages
 The accreditation body (I.e. ForHumanity) is a volunteer body which doesn't add high personnel cost to the accreditation process.	 It is expected to be higher effort for the accreditation body given they will have to manage certification of volunteers. ForHumanity is currently reviewing the standards and collecting feedback from experts which is could be a tedious process.
 The training course is free and open to anyone to become a certified assessor/auditor and the accreditation process is sector agnostic so the applicant does not need a specialised skill set.	 There is the risk of quality of assessment given there is a low barrier to entry to become an auditor, and no clear requirements to renew the training once certified. There is also the risk of inconsistent or low quantity of trained assessors are available due to voluntary basis of work.
 This is a global approach and sector agnostic, which makes it inclusive and applicable to a wide range of AI systems and autonomous services.	 Not much information available about the the full process and requirements.
 Applicants apply online and assessment is conducted remotely/online allowing for an global approach.	 The scheme is undergoing review, which means certain operations and processes are not determined such as suggested renewal date and process review.
 Volunteers can be based anywhere and can provide regional knowledge in understanding different markets across industry.	

Third-Party Accreditation

Cyber Assessment Framework (CAF)

Cyber Assessment Framework (CAF)

Approach type: Third-party accreditation

Approach Summary

A **regulated accreditation process** for Critical National Infrastructure (CNI) bodies, and other relevant organisations, that provides a systematic and **comprehensive approach to assessing how organisation manage cyber risks to the essential functions of their business/service**. Assessments are conducted by an NCSC-authorized accreditation body.

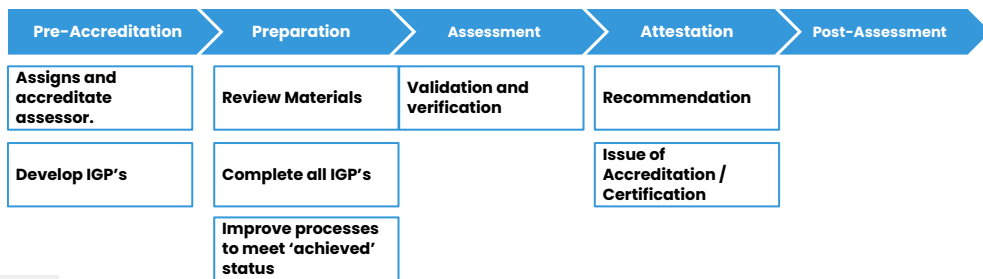
Sector	Geography	Accreditation Body	Standards Body
		 National Cyber Security Centre	  National Cyber Security Centre

Necessity: Regulated by NCSC

Standards: Standards across IEC, ISO, NCSC, and are aligned with individual principles. See the [table view](#) for full list.

Key Assessment Criteria

Process overview



Technical/Non-Technical. Organisations must meet all 'achieved', and in some cases 'partially achieved' outcomes as outlined in the Indicators of Good practice (IGP) Table per principle. The precise approach organisations adopt to achieve each principle will vary according to organisational circumstances.

The process requires involvement from multiple parties and high efforts to review and comply with over 88+ standards and guides PUBLIC



Sets standards and guidance. See full list [here](#) (88+).



Assigns and **accreditate authorised assessor**. Aligns standards with each principle and **develop Indicator of Good Practice (IGP) Tables**.

Communicates with applicant during the process.

Trained assessor **reviews IGP's and evidence**.

Provides **recommendations** for improvement or **issues certification**.

Specific Service (CNI bodies, and other relevant organisations)



Reviews all materias, particularly the Indicators of Good Practice and standards per principle. **Completes all IGP's**, aiming for 'achieved' or where applicable, 'partially achieved'.

Submit the final IGP's alongside evidence meeting standards per principle.

CAF adopts a highly regulated approach that requires considerable resource allocation

PUBLIC

Advantages	Disadvantages
 A specialised skill set from applicants is not required to complete the IGP's.  The information around IGP's, principles, and standards are presented in a digestible format on the website for independent learning.  The framework is applicable across a wide range of CNI and government bodies, and is easily replicable across sectors.	 Given the amount of standards and principles, as well as outcomes or outputs per Indicator of Good Practice (IGP), it can be expected both applicants need high effort and time to complete all 39 self-assessments and update processes as needed.  The assessor will need to review all evidence of each IGP (39 total) and will require an extended period of time for assessment.  A specialised skill set may be required by the auditor to understand sector specific evidence as well as meeting technical standards requirements.  UK regulation specific and dependent and therefore there may be contextual and legislative nuances specific to this approach.  Given it is regulated, the accreditation body must manage a large volume of applications and therefore ease of maintenance can be hindered given consistent stream of applications.  Renewal and internal review processes were not strictly stated.



Time/Effort



Cost



Staffing/Skills



Transparency



Scalability



Ease of Maintenance

Third-Party Accreditation

TEMPEST and EMS Accreditation Scheme

TEMPEST and EMS Accreditation Scheme

Approach type: Third-party accreditation

Approach Summary

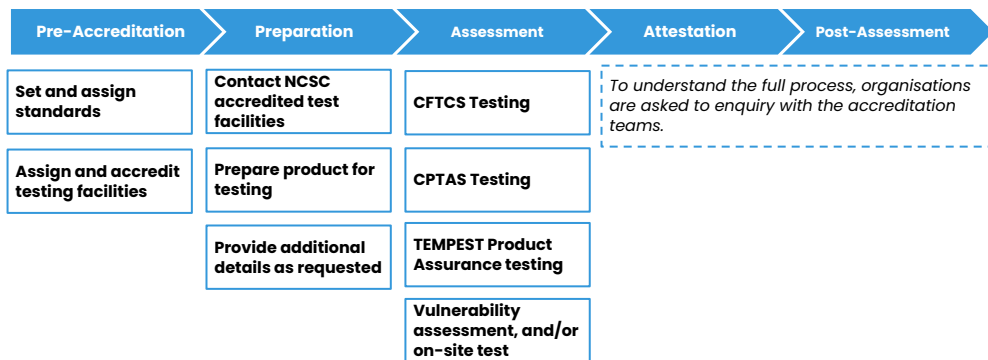
This cybersecurity scheme **manages and assesses the potential exploitation of electromagnetic vulnerabilities in ICT infrastructure**. The scheme consists of two parts: the formal scheme for all products (CFTCS) and a mobile device scheme for the First of Type assessment (CPTAS). Conformity assessments are conducted by a qualified team of engineers and/or designated test facilities.

Sector	Geography	Accreditation Body	Standards Body
		 National Cyber Security Centre NCSC accredited testing facilities	 National Cyber Security Centre

Necessity: Regulated by NCSC

Standards: NATO and EU TEMPEST and EMS standards

Process overview



Key Assessment Criteria

Technical. Technical Assessment criteria is dependent on each scheme:

1. CFTCS – Formal TEMPEST Certification Scheme for certifying products: CFTCS standards
2. CPTAS – Platform TEMPEST Accreditation Scheme for TEMPEST testing of mobile platforms

Additionally, products undergo TEMPEST Production Assurance Testing.

Assessment is performed in an NCSC-accredited testing environment and may include on-site testing

PUBLIC



Standards Body Set standards.



Variably, provide TEMPEST and EMS Operational **Assurance** and **Consultancy**.

Variably, conduct a **vulnerability assessment, visual inspection** and/or in-depth **on-site testing** at a customer's installation.

Accreditation Body



Assign **and accredit testing facilities** per scheme. **Assign standards** per scheme.

NCSC accredited testing facilities

Assign assessor and **communicate requirements** to applicant.

Conduct **CFTCS or CPTAS testing**. Conduct **TEMPEST Product Assurance Testing** to ensure consistent build standard.

Issue **report** and **certification**.

Technical Product



Contact NCSC accredited test facility. Prepare the product for testing. Provide additional **evidence, data, or information** as requested

Apply for further accreditation **per technological product/system**.

The TEMPEST and EMS approach is valuable for understanding and managing specific technology vulnerabilities

PUBLIC

Advantages	Disadvantages
 This process is sector agnostic and is able to be scaled across many industries.  Applicants can apply per system and product allowing for flexibility in regards to personalisation of accreditation across all systems, products, services, etc.	 To conduct three different technical testings across two testing facilities, the accreditation body will need a high effort and longer length of time to complete the process.  Technical testing at laboratories will incur a high expense given the technical requirements for appropriate testing: technical systems, equipment, and technical experts/engineers.  A specialist skill set is required for both the applicant and accreditor due to highly technical standards and systems/products.  The applicant is asked to contact the testing facilities to understand the details of the process including requirements, standards, and more.  UK regulation specific and dependent and therefore there may be contextual and legislative nuances specific to this approach.  High level of effort in changing and adapting testing facilities site given they are decentralised and would require an update on equipment and systems.

Third-Party Accreditation

B Corp Certification

B Corp Certification

Approach type: Third-party accreditation

Approach Summary

A five-step accreditation process to assess business sustainability adhering to social and environmental standards. The country chapters act as the accreditation body owner, while B Lab Global office sets standards and verifies results. B Lab provides key resources and networking events to continue learning and engagement after certification. Businesses are required to re-apply for B Corp accreditation every 3 years.

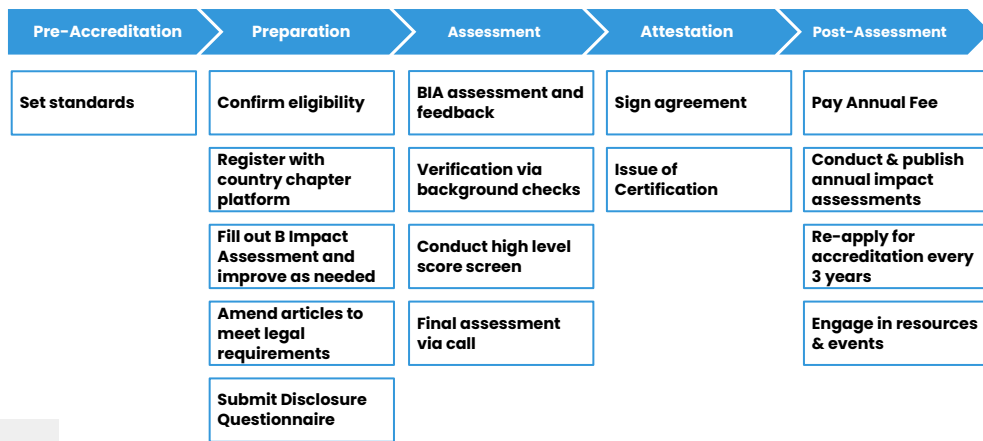
Sector	Geography	Accreditation Body	Standards Body
			

Necessity: Voluntary

Standards: Standards set by B Corp Global Standard Advisory council and are aligned with UN SDG's

Source(s): [How to certify as a B Corp](#); [A Guide to B Corp Certification](#)

Process overview



Key Assessment Criteria

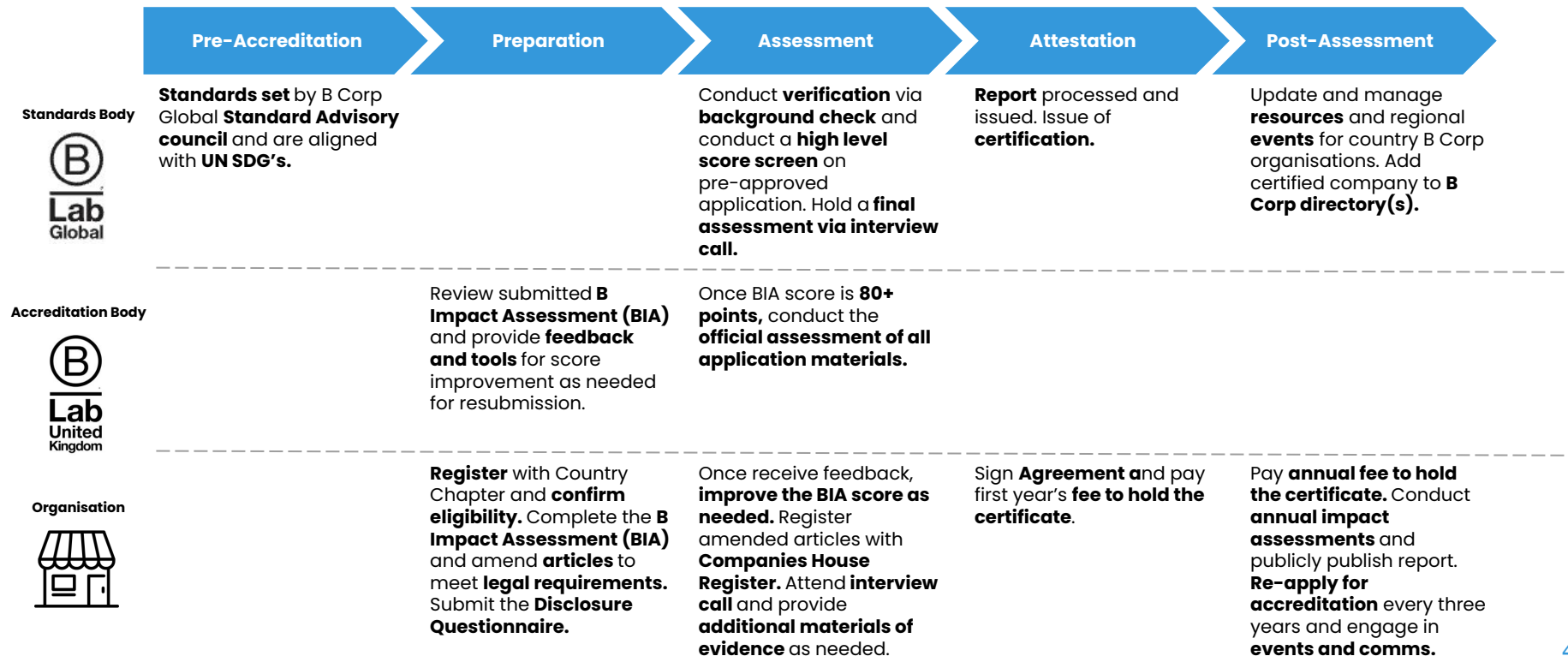
Non-Technical. During the Impact assessment companies are assessed on:

1. Business operations
2. Business model across 16 standards grouped in five impact areas: **Governance, Workers, Environment, Community, Customers.**

Companies' articles are reviewed to ensure appropriate legal language is adopted aligning with sustainability. To be eligible companies must be for profit operating in a competitive market for at least 12 months.

Responsibility is shared between B Corp Global and country chapters to review accreditation

PUBLIC



Source(s): [How to certify as a B Corp; A Guide to B Corp Certification](#)

B Corp Certification is a highly scalable approach as the reach is global and product/sector agnostic

PUBLIC

Advantages	Disadvantages
 Companies can dedicate one part-time employee to complete the process over the period of application.  Shared responsibility between global and country based chapters allows to effectively process large volumes of applications on a global scale.  Cost is dependent on the size and revenue of the company.  Little technical or specialist expertise is required for both applicants and assessors.  Very clear process and user friendly interface for applicants to foster independent learning and application.  Many resources and learning tools are provided for the application before and during the application process. There are also opportunities for continuous engagement and learning following the accreditation.  Global and country chapter for regional specialism and industry knowledge.  Requires renewal of accreditation every three years and requires companies to conduct annual impact reports to track progress demonstrating continuous review of their process.  B Corp Global produces an annual impact report indicating annual reviews of their accreditation process.	 Due to more hands-on approach, assigned advisor from country chapter may spend longer periods of time assisting applicant to improve their BIA score and amend their article's language.  Applicants may spend longer periods of time on BIA score, and improving processes if they do not complete minimum score to begin with. The average timeline varies between a few months a year.  Consistent stream and volume of applications requires a FTE larger team to appropriately handle assessment and support.  Only specialism or technical expertise is required for the legal review to assist companies in amending legal language in articles.

Third-Party Accreditation

The LEED Certificate

The LEED Certificate

Approach type: Third-party accreditation

Approach Summary

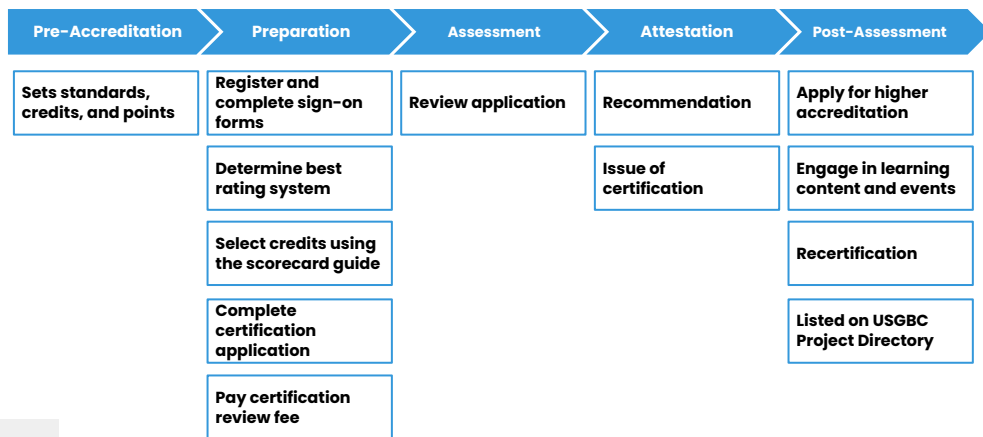
LEED **provides a framework and certification programme recognising sustainable buildings.** The conformity assessment is carried out by the Green Building Certification Incorporation (GBCI), founded specifically for independent assessment and project certification for LEED. **The certification is a tiered, points-based approach** allowing variance levels of recognition for projects achieving some to all of the standards.

Sector	Geography	Accreditation Body	Standards Body
		 GBCI	

Necessity: Voluntary

Standards: Standards are specified per building type (ie. hospitals, historical, etc.), and align with the UN SDGs

Process overview



Key Assessment Criteria

Non-Technical. To achieve LEED certification, a project earns points by adhering to prerequisites and credits that address carbon, energy, water, waste, transportation, materials, health and indoor environmental quality as outlined in the standards.

Project select specific rating systems and certification scheme based on their project categorisation. This will determine the credit point assessment.

USGBC established the Green Business Certification Inc. to be the independent body for reviewing and accrediting projects

PUBLIC

Pre-Accreditation

Preparation

Assessment

Attestation

Post-Assessment

Standards Body



Sets standards, credits, and points per certification version and rating system.

Host **resources** and **events** to engage community, including the **annual Greenbuild International Conference**.

Accreditation Body



Provides **learning resources** and **guiding tools**, such as the **scorecard** for applicants.

Application is reviewed and assessed by Green Business Certification Inc (GBCI). **Verification** conducted by GBCI.

GBCI issues certificate to appropriate **LEED Level**: Certified, Silver, Gold or Platinum.

GBCI®

Non Technology Product



Register and determine **best rating system** for project. Completes **sign-on forms**. **Reviews and selects the credits** to pursue. Completes **certification application** and provides evidence as needed. Pays a **certification review fee**.

Engages in **events** and **learning resources**. **Reapplies** for **higher certification**, and applies for **recertification** as needed.

Source(s): [LEED Rating System](#) ; [LEED Scorecard](#)

LEED deploys a unique tiered, points-based approach to accreditation PUBLIC putting the onus on applicants to select correct rating systems and schemes

Advantages	Disadvantages
 Project teams can dedicate one part-time employee to complete the process over the period of application.  Project teams do not need a specialist skill set or expertise in sustainability to complete the application. The scorecard is provided for ease of understanding the credit and review system.  While there are many rating systems, the tools and guidance assist applicants in choosing the best fit process for their project and foster independent learning.  USGBC provides learning materials online before, during, and after the application process.  The scheme is globally recognised and applies across multiple sectors and project types.  USGBC produces an annual report on green building impact demonstrating continuous review of their process.  If applicable, applicants can apply for higher accreditation. The tiered approach allow for SMEs to certify project sustainability as they mature or their industry changes.	 Dedicated FTEs are required to ensure smooth onboarding, assessment, and continuous engagement of applications. Given the consistent and large volume of applications, the assessment is a full time responsibility for accreditation body.  Applicants are required to pay to apply, even if they do not receive an accreditation.  A team of sectoral-specific experts is required for each rating system given the specificity of assessment per project type.  Given there are versions and ratings systems or legislation specific to project type, changes in the industry may require an update to theses rating types which would require higher levels of maintenance (ie. change in carbon emission regulation).  There may be a risk that given there are different levels of certification, the lowest level may be perceived as inadequate or illegitimate, comparatively to the higher levels of accreditation.

Third-Party Accreditation

EASA Part 145 Accreditation

EASA Part 145 Accreditation

Approach type: Third-party accreditation

Approach Summary

Overview: Part 145 is the European standard for the approval of organisations that perform maintenance on aircraft and aircraft components that are registered in EASA Member States. The accreditation will be carried out by each jurisdiction aviation authority of EASA member States.

Sector	Geography	Accreditation Body	Standards Body
			

Necessity: Regulated

Standards: Regulation (EU) No 1321/2014

Process overview

Pre-Accreditation	Preparation	Assessment	Attestation	Post-Assessment
Approves standards	Readiness Assessment tool and application	On-site assessment	Recommendation	Renewal of accreditation
Incorporated processes and regulation	Documentation review	Testing	Declaration of conformity	Suspension / Revocation

Technical/Non-Technical.

Key Assessment Criteria

1. **Facilities:** Must have facilities commensurate with the scope of work for which it is approved to provide.
2. **Maintenance Data:** Generic Maintenance data for each aircraft type within the requested or approved scope must be available at all times.
3. **Tooling and equipment:** Organisations must have all tooling which is required to complete the maintenance tasks within their scope of work permanently available at their facilities.
4. **Manpower resources:** The organisation shall have sufficient staff to plan, perform, supervise, inspect and quality monitor the activities which the organisation is approved to perform.
5. **The Maintenance Organisation Exposition (MOE):** The MOE is integral to an organisation's ability to demonstrate its capability and compliance with Part 145.

The process requires local aviation authorities to perform the accreditation following EASA standards

PUBLIC

Pre-Accreditation

Preparation

Assessment

Attestation

Post-Assessment

Standards Body



Approves standards for accreditation of organisations providing maintenance.

Accreditation Body



Incorporated **processes and regulation** from EASA regulation into **national legislation**.

Performs an **on-site audit** of the organisation and **reviews application**.

Local aviation authority submits their **recommendations** and **grant authorisation**.

Organisation providing maintenance



Submits an **application form** which includes **documentation** and **information** set by specific regulation. **Pays** relevant fee for accreditation.

Notified of authorisation approval or rejection.

EASA Part 145 authorises experts to certify aircraft maintenance and harmonises standardisation efforts across regulation

PUBLIC

Advantages	Disadvantages
 This is a standard approach to the accreditation of entities that will provide aircraft maintenance, meaning that the approach is giving transparency to organisations that the maintenance is provided by certified and competent organisations and individuals.  The approach is harmonised with other types of legislation in a heavily regulated industry.	 Due to the type of accreditation involved, the documentation required is extensive.  High levels of expertise and skills are required to go through the audit process and on-site visit both for the organisation and accreditation body.  There is limited information available on EASAs website about the process and on-site visit audit.



Time/Effort



Cost



Staffing/Skills



Transparency



Scalability



Ease of Maintenance

Source(s): PUBLIC Analysis

Mixed Accreditation

Digital Technology Assessment Criteria (DTAC)

Digital Technology Assessment Criteria (DTAC)

Approach type: Mixed

Approach Summary

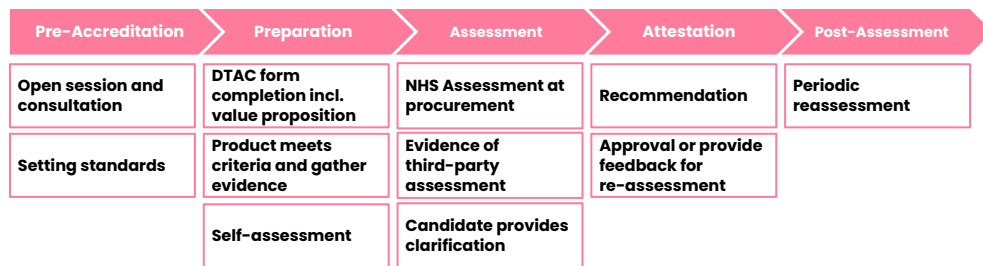
An assessment criteria for **digital health technologies entering and already used in the NHS and social care**. It is used by healthcare organisations to **assess suppliers at the point of procurement** or as part of a due diligence process, to make sure digital technologies meet minimum baseline standards. For developers, it sets out what is expected for entry into the NHS and social care.

Sector	Geography	Conformity Assessment Body	Standards Body
			 

Necessity: Voluntary

Standards: Combination of existing legislation (GDPR, DCB0129 and DCB0160) and best practice

Process overview



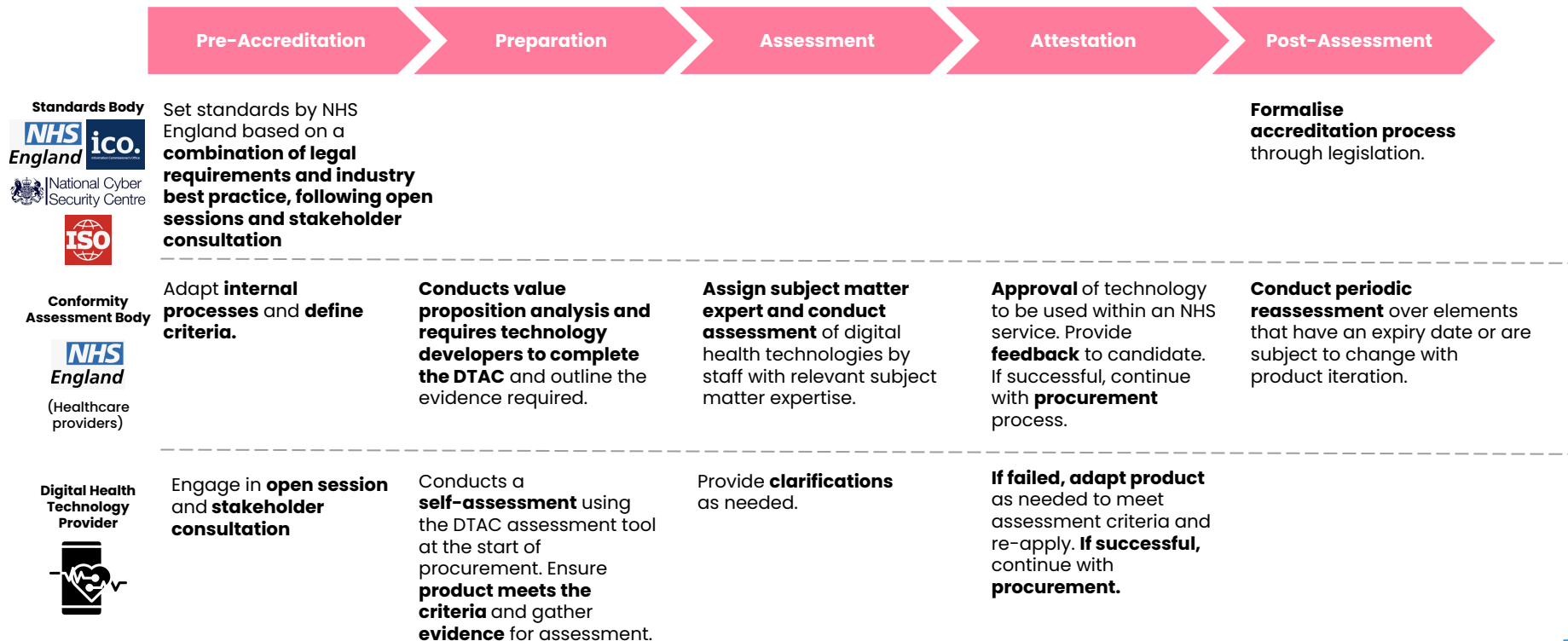
Key Assessment Criteria

Technical/Non-Technical.

- Clinical safety:** Products are assessed to ensure that clinical safety measures are in place and that organisations undertake clinical risk management activities to manage this risk.
- Data protection:** Products are assessed to ensure that data protection and privacy is 'by design'.
- Technical assurance:** Products are assessed to ensure that products are secure and stable.
- Interoperability:** Products are assessed to ensure that data is communicated accurately and quickly whilst staying safe and secure.
- Usability and accessibility:** Products are allocated a conformity rating having been benchmarked against good practice and the NHS service standard.

Healthcare technology are assessed on meeting the minimum baseline standards through self and third party reviews

PUBLIC



DTAC approach to assess technologies used in healthcare technology procurement improves supply chain confidence

PUBLIC

Advantages	Disadvantages
 Organisations can download the DTAC form from the website and most of the questions have a yes/no answer format, reducing time and effort spend on completing the questionnaire.  Self-assessment tool and DTAC forms are available to download from the NHS website. Organisations do not need to incur in additional cost unless they want to hire a third party to conduct independent assessment.  Simple and clear questionnaire format allows for minimum resources allocation to complete application.  NHS offers both pre-assessment and training support for organisations who want to go through the assessment. This will facilitate familiarity with the process and timelines.	 NHS suggests that as part of each new procurement process or contract renewal, buyers of digital health technology should ask the developer to complete the DTAC, which can could delay procurement processes.  NHS suggests that those with relevant subject matter expertise in the healthcare provider side are involved in the assessment of digital health technologies, which means utilising qualified resources to assess specific sections of the assessment.  DTAC is a common baseline criteria in terms of safety and security, but it is only one part of procurement – it is not intended to be the complete question set for procurements and should be supplemented with additional specifications, reducing predictability for technology developers.

Mixed Accreditation

Singapore's Approach to AI Governance

Singapore's Approach to AI Governance

Approach type: Mixed

Approach Summary

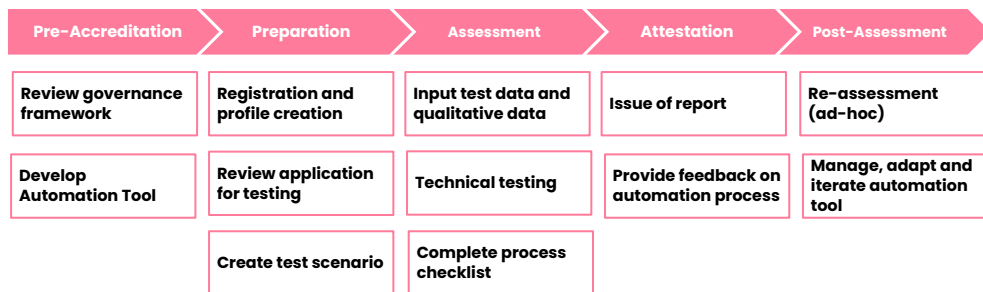
Singapore's **AI accreditation process involves companies registering with the government's platform**, AI Verify, to assess their alignment with the AI Model Framework Principles. The AI Verify tool provides a governance testing framework to understand the process and a software toolkit to conduct the conformity assessment. AI Verify tool and the framework are currently under consultation and in the MVP stage.

Sector	Geography	Accreditation Body	Standards Body
			

Necessity: Voluntary

Standards: Eight of the eleven PDPC's AI Model Framework Principles

Process overview



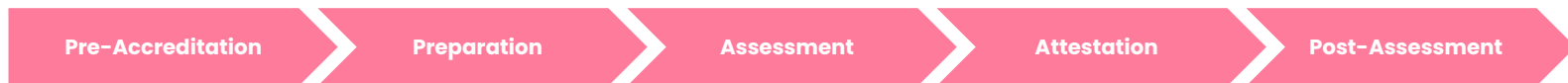
Key Assessment Criteria

Technical/Non-Technical. The AI Verify MVP conducts assessment for 8 of the 11 principles.

- For Fairness, Robustness, and Accountability, a combination of technical testing and process checklists, where companies document key considerations including rationale, trade-offs, risk assessments, and other feedback relevant to the industry, are required.
- For Transparency, Explainability, Repeatability/Reproducibility, Safety, and Human Agency & Oversight, only process checks (non-technical) are required.

The user-friendly interface of AI Verify provides clarity on process steps, timelines and status

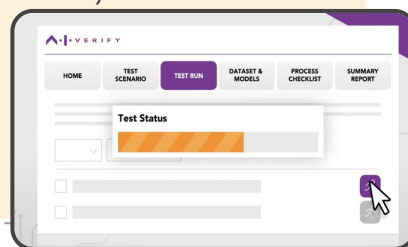
PUBLIC



Standards Body

Set out principles / standards in the Model AI Framework.

AI Verify Interface



Update of AI standardisation and stakeholder engagement.

Accreditation Body

Developed AI Verify Tool.

AI Verify Tool **guides** application through process. **Reviews application** for testing.

AI Verify Tool **runs technical testing** and assesses **process checklist** data.

Issue assessment reports.

Manage and update AI Verify platform based on **consultation feedback.**

Organisation



Review the **governance framework** and supporting materials.

Register with the AI Verify Tool. **Create test scenario** and **clean datasets.**

Provide documentation required for process checks. **Install and initialise testing scenarios. Adjust parameters** and **input datasets.**

Provide feedback to IMDA on process and AI Verify.

Conduct reassessment with AI Verify as desired. **Continuous engagement** for scheme iteration.

Automated assessment tools helps promote scalability, with the potential to be replicated across markets and regions

PUBLIC

Advantages	Disadvantages
 The assessment is run via an automated assessment tool, including technical testing which therefore does not require manual labour or review by a FTE.  The organisation can complete the application and run the software independently in a short period of time (estimated less than 2 hours based on demo).  No expertise is required from the applicant to understand complex standards or accreditation as the workflow guides applicants through the process.  Organisations can learn and complete the entire assessment independently and information is provided in multiple formats: i.e. written framework, video guides, interactive workflow/configure test, etc.  The technology is sector agnostic and can be applied to any AI dataset, services and companies using AI. The testing is done via platform accessible on the Open Web (as of yet).  Currently, there is a high level of engagement across industry to inform and test the build for the AI Verify tool.  Organisations can run reassessment to their needs.	 The PDPC/IMDA team incurred up front developer and engineering costs to build and test the framework and the software to ensure accuracy and effectiveness.  A team of skilled engineers would be required to build the AI Verify software and continue adapting and testing.  Additional expertise in testing AI dataset for the technical assessment would be required at set up and periods of review.  The exact ease of maintenance is uncertain as processes have yet to be determined (ie. review process, renewal, etc.).

Mixed Accreditation

Cyber Essentials/Cyber Essentials Plus

Cyber Essentials/Cyber Essentials Plus

Approach type: Mixed

Approach Summary

Government-backed scheme that helps organisations **assess their cyber risk** and **build processes to protect** themselves. There are **two levels of certification**:

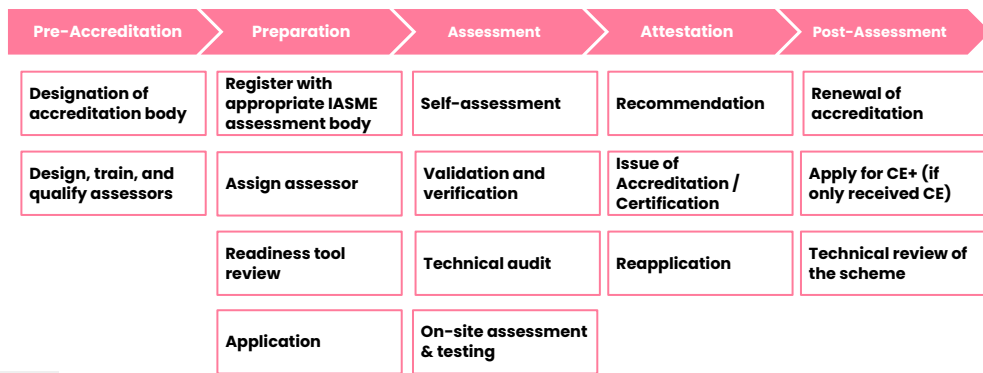
1. **Cyber Essentials (CE)**: Self-accreditation process
2. **Cyber Essentials Plus (CE+)**: Self-accreditation process coupled with a third-party technical verification

Sector	Geography	Accreditation Body	Standards Body
			 National Cyber Security Centre

Necessity: Varies

Standards: NCSC five basic security controls

Process overview



Key Assessment Criteria

Technical/Non-Technical. Reviewing and assessing across the five basic security controls: (1) firewalls: use a firewall to secure your internet connection; (2) secure configuration: choose the most secure settings for your devices and software; (3) user access control: control who has access to your data and services; (4) malware protection: protect yourself from viruses and other malware; (5) security update management: keep your devices and software up to date.

The process is well-structured with clear assessment criteria for CE/CE+, however it requires high burden on CE+ applicants

PUBLIC

Pre-Accreditation

Preparation

Assessment

Attestation

Post-Assessment

Standards Body Set standards.



Accreditation Body **Accreditate and designate IASME members** to carry out scheme. Identify **technical expert for CE+ technical assessment.** * **Train and qualify** assessors.



Provide application with access to certification information and **assign assessor and/or technical expert.***

IASME qualified assessor **reviews submitted self-assessment.** Technical expert conducts **technical audit of IT systems** and performs an on-site visitation for testing. *

Issue report and if failed, **provide feedback** to applicant. If/once successful will **issue certification.**

Conduct ongoing **regular review of the CE/CE+ scheme.** As part of the review, NCSC and IASME **updates technical requirements.**

Organisation



Review the **CE Readiness toolkit.** Last **CE** was completed **within 3 months.*** **Register** with appropriate **IASME member.** Pay **application fee.**

Conduct **Self-assessment.** Company **board member signs the declaration.** Grant **access to technical material** as requested by technical expert.*

Receive feedback to **improve processes.**

Reapply for CE, if failed. If successful, can **bid for sensitive central government contracts.** **Renew accreditation** on an annual basis. CE certified bodies can **apply for CE+ certification.**

**Note: Applicable for Cyber Essentials Plus only.*

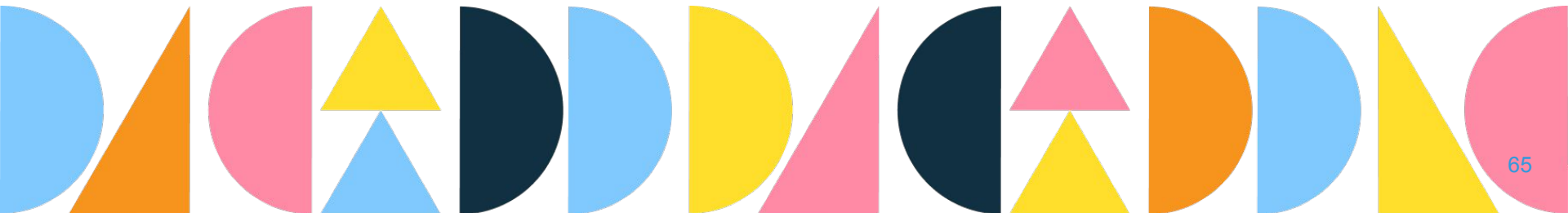
Source(s): [About Cyber Essentials](#) ; [Get ready for CYBER ESSENTIALS](#)

CE/CE+ adopts a highly flexible approach to give organisations the optionality of self assessment or third party verification

PUBLIC

Advantages	Disadvantages
 For CE, a simple review and verification process is required by the assessor , while most of the manual labour is carried out by the applicant themselves.	 High level of effort is needed to run the technical audit for CE+ as it requires an on site testing for internal and external networks and systems.
 For CE, organisations can independently complete the self-accreditation process with little needed speciality in skills, and can designate one FTE over short period of time.	 Minimum charge for application is £300 and is based on the organisation size.
 The Cyber Essentials Readiness Toolkit assists companies in understanding all requirements and acts as a checklist before undergoing the formal assessment process.	 Accredited bodies must designate a technical expert for CE+ , and expected resourcing is higher given an on-site testing process is conducted which could cause high cost for staffing.
 The process is sector and technology agnostic and applies to a wide range of subjects (services, systems, product, and organisations). Given this wide approach it can be iterated across many contexts and industries.	 Technical expertise is required to carry out the assessment for CE+ . Depending on the subject type, expertise in sectors and industry may be required.
	 To understand the specifics assessment standards for CE+ technical audit, organisations must contact the IASME member directly and get a quote .
	 Given it can be applied to a wide range of subjects, there may be high frequency of change across both industry and regulation in which would require a review and potential update of the process of each applicable IASME Member.

Further Insights: Deep Dive Case Studies



PUBLIC and Ofcom prioritised 3 representative approaches across different sectors for deep-dive case studies

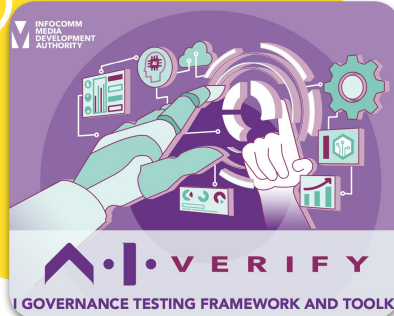
01

NHS England - Transformation Directorate



**Digital Technology
Assessment Criteria
(DTAC)**

02



**Singapore's AI
Governance Testing
Framework and Toolkit**

03



**Cyber Essentials
Scheme**

Through deep-dive analysis, we summarised key commonalities, advantages and disadvantages of three approaches

	NHS' Digital Technology Assessment Criteria (DTAC)	Singapore's AI Governance Testing Framework and Toolkit	NCSC Cyber Essentials Scheme
Common Themes	• Mixed, principles based approaches facilitate flexibility and adaptability to applicants' needs and changing circumstances. • Process/documentation check is layered with technical testing to promote comprehensive assessments. • Assessment criteria are made publicly available and accessible to help applicants prepare for accreditation early.		
Key Advantages	• Builds on a mix of regulations, standards and industry best practice. • Uses simple, clear, transparent questionnaires for self-assessment to reduce the burden on applicants and enable high scalability. • No application cost as DTAC requires no accreditation prior to the NHS technology procurement process.	• Aligns with international AI principles and promotes international collaboration. • Early and continuous engagement with tech industries, AI testing community, standards bodies and regulators, to pilot and test the toolkit. • The automated assessment process enables rapid, streamlined self-assessment and high scalability. • Sector agnostic with the potential to be applied to all AI systems.	• The two-pronged approach provides applicants flexibility and optionality to choose the level of compliance. • The tiered pricing structure ensures accessibility and affordability for businesses of all sizes. • IASME is a singular accreditation partner to provide a clear and consistent pathway for applicants. • Regular review of the scheme by NCSC and IASME to ensure adaptability to changing nature of technologies.
Key Disadvantages	• Potential risks of delayed procurement processes. • DTAC only forms baseline criteria of safety and security and needs to be assessed together with other specifications.	• High upfront cost and resource requirements to build, test and adapt the framework and develop the automated assessment software. • This approach is currently under piloting and testing, with limited evidence of its effectiveness at scale.	• Uptake and awareness of the scheme remains low for micro and small organisation. • High resource/sector expertise requirements on the assessor and CE+ applicants to run technical auditing.

NHS

Digital Technology Assessment Criteria (DTAC)

NHS's Digital Technology Assessment Criteria (DTAC) ensures digital technologies to meet minimum baseline standards

NHS implemented* the DTAC **assessment criteria for digital health technologies** entering or already used in the NHS. It gives **staff, patients and citizens confidence** that the digital health tools they use are safe

CRITICAL SUCCESS FACTORS



Confidence

- **Builds on existing NHS and other regulations, standards and processes**
- **Incentivises uptake with minimum safety, technical and usability criteria**, while reducing the burden to both developers and assessment bodies.



Simplicity

- Assessed in **simple, clear questionnaire format** to **reduce burden** on developer.
- Equips local and national NHS with a **simple decision-making tool for tech adoption**.



High flexibility / accessibility

- DTAC **brings together other best practice standards into a single approach** making it flexible
- **Easily adapted to new forms of technology** within the healthcare industry, either on piloting or testing phases.

LIMITATIONS

- **Lack of legislative framework** for the DTAC, which means that it is used only as guidance for local healthcare providers who want to buy technology.
- Commonly used assessment method for digital suppliers but **uptake thresholds are not standardised** across local healthcare providers

***Note:** NHS first introduced the DTAC in beta in October 2020, and incorporated feedback before launching the first official version in February 2021

Source(s): [Digital Technology Assessment Criteria \(DTAC\)](#), [NHS bodies asked for 'action plans' to ensure tech suppliers meet standards](#) | [PublicTechnology.net](#)

The first 4 sections of the DTAC form the technical assessed criteria...

DTAC's 4 technical assessment criteria uses pass or fail assessment to determine the overall success of the product or service

Technical Assessment Criteria

Criteria	Standard(s)	Assessment Method
Clinical safety: Establishing that the product is clinically safe to use	• DCB0129 standard (which applies to technology developers) • UK Medical Device Regulations 2002 (MDR 2022)	To pass, the developer is required to: • Confirm they have undertaken Clinical Risk Management activities in compliance with DCB0129 • Provide evidence that a clinical risk management system is in place and that it is compliant with the requirements set out in DCB0129. • Submit a Clinical Safety Case Report and Hazard Log compliant with DCB0129 requirements • Name a CSO which can be through an outsourced arrangement • Confirm that the product is registered with the MHRA if in scope of MDR 2022 • Provide documentation about risk classification of the product if in scope of MDR 2022 • Provide a valid conformity certificate in accordance with DCB0129 if the product connects to any third-party products
Data protection: Establishing whether the product collects, stores and uses personally identifiable data compliantly	• UK GDPR • Data Security and Protection Toolkit	To pass, the developer is required to: • Submit evidence that they have a registration with the ICO or that they do not require one • Confirm they have a DPO in place where this is mandated or that they are not required to do so. • Confirm that they are compliant with the Data Security and Protection Toolkit Assessment • Provide a Data Protection Impact Assessment that is compliant with the GDPR • confirm that their Data Protection Officer has signed-off the risk assessments and mitigations, access controls and system level security policies • Confirm where the developer stores and process data (UK, EU or outside of EU) and demonstrate that the country in which the data is processed or stores is compliant with current legislation.

... these ensure that the product or service is safe to be used by staff, patients and citizens

These criteria will determine the overall success of the assessment of the product or service

Technical Assessment Criteria

Criteria	Standard(s)	Assessment Method
Technical security: Establishing that the product meets industry best practice security standards and that the product is stable	Cyber Essentials Penetration Testing with no vulnerabilities that score 7.0 or above using the Common Vulnerability Scoring System (CVSS)	To pass , the developer is required to: • Have a valid Cyber Essentials certificate • Evidence that the product has undergone an external penetration test that includes the OWASP top 10 vulnerabilities • Confirm that an internal or an external custom code security review has been undertaken in accordance with NCSC guidance • Confirm that all privileged accounts have Multi Factor Authentication in accordance with NCSC guidance • Confirm that logging and reporting requirements have been clearly defined • Confirm that load testing has been performed
Interoperability criteria: Establishing how well your product exchanges data with other systems	• ISO/IEEE 10073 • API guidance issued by NHS and GDS • NHS Login	To pass , the developer is required to: • Demonstrate that the product have API's follow Government Digital Services Open API Best Practice, are documented and freely available, and that third parties have reasonable access to connect. • Confirm that if a product uses an NHS number to identify a patient record, that it uses NHS Login • Confirm that the product has the capability to read/write into Electronic Health Records using industry standards for secure interoperability (i.e. OAuth 2.0, TLS 1.2) • Evidence compliance with ISO/IEEE 10073

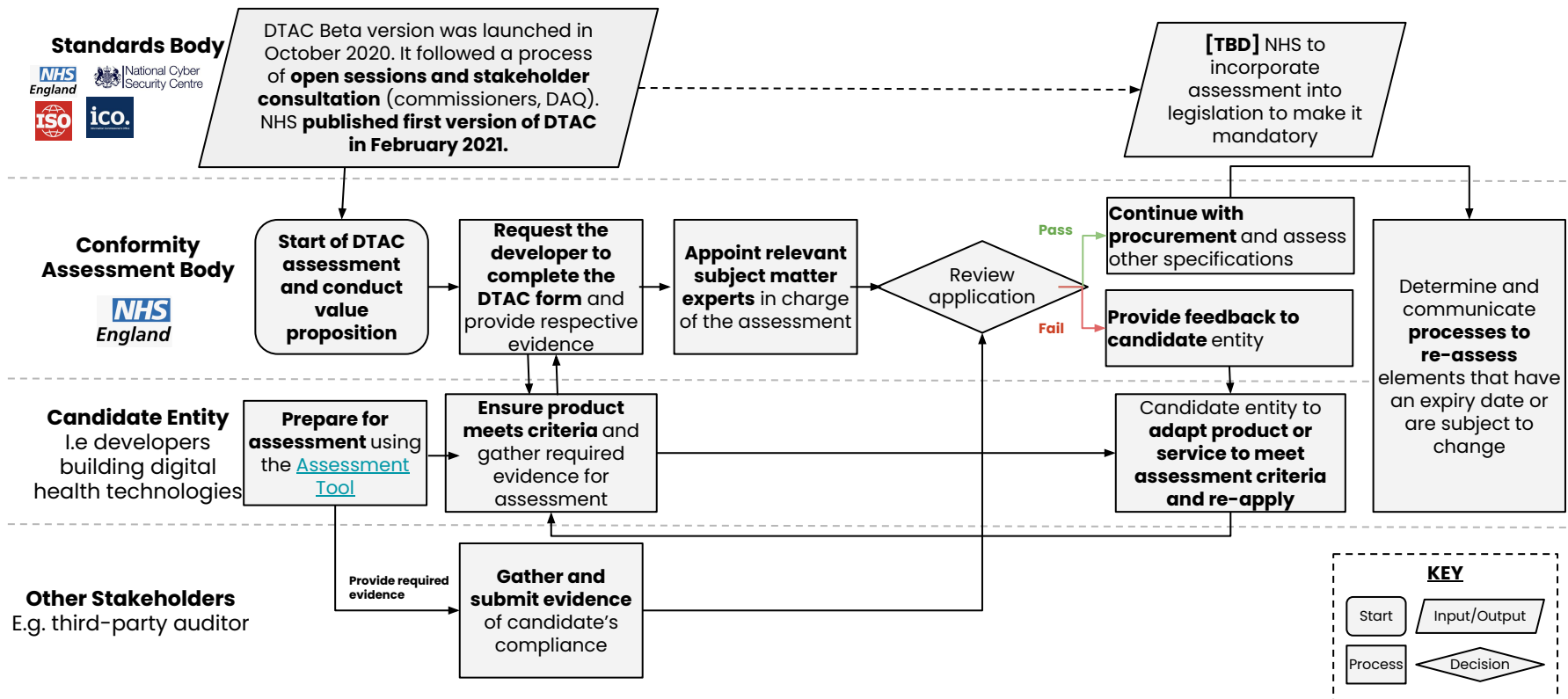
Section 5 of DTAC is targeted at ensuring that the product or service is suitable for use

*This assessment sets a **compliance rating**. This assessment does not contribute to the overall Assessment Criteria as set out*

Non-technical Assessment Criteria

Criteria	Standard(s)	Assessment Method
Usability and accessibility: Establishing that the product has followed best practice	• NHS service standard • WCAG 2.1 level AA • Government Digital Service (GDS) guidance accessibility and accessibility statements	The non-technical assessment criteria is scored against the NHS service standard Developers are required to demonstrate: • User need has been taken in account through user research, search data, analytics or other data to understand the problem; • Working towards solving a whole problem for users; • Making the service simple to use (i.e. by showing user acceptance testing to validate usability of the product); • Complying with WCAG 2.1 level AA and publishing accessibility statement • Having a multidisciplinary team; • Using agile ways of working; • Iterating and improving frequently; • Defining what success looks like and being open about how the service is performing; • Ensuring the product meets cloud first and / or internet first; • Using and contributing to open standards, common components and patterns; • Offering a service level agreement, reporting on performance and having an uptime of 99.9% or above.

The DTAC is designed to provide clear guidance on how to build and buy fit-for-purpose digital health technologies



Developers are responsible for meeting DTAC criteria and providing evidence, while the NHS ensures compliance

RACI Matrix	Pre-Accreditation Preparation Assessment Attestation Post-Assessment									
	Definition of assessment criteria	Readiness self assessment	Application for procurement	Value Proposition	Appointment of subject matter expert	Evidence and documentation review	If pass: continue with procurement	If fail: provide feedback and re-apply	Periodic reassessment	Formalisation of accreditation process
Standards Body    	R	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A R
Conformity Assessment Body 	A R	N/A	I	A R	A R	A R	A R	A R	R	R C
Candidate Entity i.e. developers building digital health technologies	C	A R	A R	R	I	R	I R	I R	A R	C (TBD)
Other Stakeholders E.g. third-party compliance services	C	R	C	R	N/A	A R	I	I	N/A	N/A

KEY

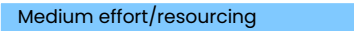
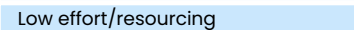
- A** Accountable: Those who are ultimately accountable for the correct and thorough completion of the deliverable or task
- R** Responsible: Those who do the work to achieve the task. There can be several R to perform one task
- C** Consulted: Those whose opinions are sought. Two-way communication
- I** Informed: Those who are kept up-to-date on progress, often only on completion of the task or deliverable. One-way communication
- N/A** Not Applicable: Those who are not involved in the task.

01

DTAC

The DTAC is a questionnaire with yes/no answers, reducing the burden on the candidate through the assessment process

Roles by Phase	Pre-Accreditation	Preparation	Assessment	Attestation	Post-Assessment
Standards Body    	Publication of standards for developers of digital health technology	N/A	N/A	N/A	Formalise accreditation process through legislation
Conformity Assessment Body 	Adapt internal processes and define criteria	Value Proposition	Appointment of subject matter expert and documentation review	Continue with procurement or provide feedback	Determine and communicate processes to re-assess elements that have an expiry date or are subject to change
Candidate Entity i.e developers building digital health technologies	Sector expertise to inform consultation	Self-Assessment: ensure product meets criteria and gather required evidence for assessment	Wait for assessment and provide any clarifications	Incorporate feedback to re-apply, or continue with procurement	
Other Stakeholders E.g. third-party compliance services	N/A	Gather evidence and conduct audit	Provide evidence of compliance with standards	N/A	N/A

KEY
 High effort/resourcing
 Medium effort/resourcing
 Low effort/resourcing

Source(s): [Digital Technology Assessment Criteria \(DTAC\)](#), PUBLIC analysis

Singapore's IMDA/PDPC

AI Governance Testing Framework and Toolkit

02

AI
Verify

Singapore's media and data regulators have developed and piloted an innovative tool to AI governance

Infocomm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC) have launched AI Verify, a **voluntary self-assessment tool of AI systems***, to foster public trust and support the increasing use in AI.

KEY STATS

10

Organisations participated in the **minimum viable product (MVP) pilot** of AI Verify in May 2022. They include organisations such as AWS, Meta, Google, Microsoft, Singapore Airlines, among others.

CRITICAL SUCCESS FACTORS



Collaboration & iteration

- **Collaborative pilot approach** and stakeholder engagement ensures the framework and toolkit **meets user needs** and can **adapt to evolving technologies**.



Scalability via automation

- **Automated** process enables **rapid, streamlined** self-assessment, **scalability** and **accommodates high volumes**
- AI Verify is intended to be **deployed in the user's environment** and is packaged into a Docker container for **easy deployment**.



User flexibility/ accessibility

- **User-friendly interface and intuitive guides** allow organisations to navigate testing scenarios and **tailor it to their specific needs**.

LIMITATIONS

- The MVP of AI Verify is **not yet applicable to images or large models**.
- **Results may be limited and oversimplified** due to absence of human review, assessment.
- Singapore's approach is **in an early pilot phase**, and thus it is **not proven at scale**.
- **High upfront costs** are required to develop automated software.

***Note:** AI Verify is currently available as a MVP, only able to support binary classification and regression model. IMDA and will work with the industry and AI testing community to **develop third-party testing and certification in the longer term**.

Source(s): [AI Governance Testing Framework and Toolkit: Invitation to Pilot](#), [Singapore's Approach to AI Governance](#), PUBLIC Analysis

Eleven principles of AI ethics are assessed through a combination of technical testing...

Technical testing for three principles: **Explainability, Robustness and Fairness** is conducted by AI Verify's one-stop toolkit deployed in the **user's environment** that **packages widely-adapted open-source** technical testing tools

Technical Assessment

Criteria	Assessment Method i.e. technical testing	Testing Toolkits (Available on GitHub)
Explainability: Ability to understand and interpret what the AI system is doing	Technical tests are conducted to identify factors contributing to AI model's output.	• Shapley Additive exPlanations (SHAP)
Robustness: Ensuring that AI system can still function despite unexpected inputs	Technical tests attempt to assess if a model performs as expected even when provided with unexpected inputs.	• Adversarial Robustness Toolkit
Fairness (Mitigation of unintended discrimination): AI systems makes same decision even if an attribute is changed	Technical tests check that an AI model is not biased on protected or sensitive attributes specified by the AI system owner, by checking the model output against the ground truth.	• AI Fairness 360 (AIF360) • Fairlearn

Example: Explainability

Testable Criteria	For each model being developed, run explainability methods to help users understand the drivers of the AI model.
Testing Process	Perform analysis to determine feature contributions.
Metric	Features contributing to model output as obtained from technical tool
Threshold	N/A
Technical Tool	IMDA Toolkit (comprising SHAP and LIME tools)

...and a process checklist for non-technical assessment

All eleven principles are assessed through **11 process checklist against 85 criteria by an automated system.**

Non-technical Assessment

Criteria	Assessment Method (i.e. process checklist)
Explainability: Ability to understand and interpret what the AI system is doing	Check considerations given to the choice of models, such as rationale, risk assessments, and trade-offs of the AI model.
Robustness: Ensuring that AI system can still function despite unexpected inputs	Check documentary evidence and review of factors that may affect the performance of AI model, including adversarial attacks.
Fairness: AI systems makes same decision even if an attribute is changed	Check documentary evidence of having a strategy for the selection of fairness metrics that are aligned with the desired outcomes of the AI system's intended application; and the definition of sensitive attributes are consistent with the legislation and corporate values.
Transparency: Appropriate information is provided to individuals impacted by AI system	Check documentary evidence of providing appropriate information to individuals who may be impacted by the AI system (i.e. under the condition of not compromising IP, safety, and system integrity, use of AI in the system, intended use, limitations, and risk assessment)
Repeatability/ Reproducibility: Ability to replicate an AI system's results	Check documentary evidence including evidence of AI model provenance, data provenance and use of versioning tools.
Safety: Known risks have been identified/mitigated	Check documentary evidence of materiality assessment and risk assessment, including how known risks of the AI system have been identified and mitigated.
Accountability: Proper management and oversight of AI system development	Check documentary evidence, including evidence of clear internal governance mechanisms for proper management oversight of the AI system's development and deployment.
Human agency and oversight: AI system designed in a way that will not decrease human ability to make decisions	Check documentary evidence that AI system is designed in a way that will not reduce human's ability to make decisions or to take control of the system. This includes defining role of human in its oversight and control of the AI system such as human-in-the-loop, over-the-loop, or out-of-the-loop
Security: AI systems can maintain confidentiality, integrity, and availability through protection mechanisms	Check documentary evidence of team competency, evidence of conducting security risks assessment at the inception of AI system development, and security measures throughout the AI system lifecycle
Data Governance: Governing data used in AI systems	Check documentary evidence of measures to understand the lineage of data and data practices to comply with regulatory requirements and industry standards.
Inclusive growth, societal & environmental well-being: Trustworthy AI to contribute to overall growth and prosperity for all	Check documentary evidence of the broader implications of the AI system beyond its functional and commercial objectives.

Source(s): [AI Governance Testing Framework and Toolkit: Invitation to Pilot](#)

02

AI
Verify

Although not assessing AI accuracy directly, the assessment of fairness and robustness ties closely with accuracy metrics

Fairness

The assessment algorithm computes a list of fairness metrics to measure how correctly an AI model predicts among the given set of sensitive features.

Robustness

The assessment plugin generates a perturbed dataset using [boundary attack](#) algorithm on the test dataset.

Relevance to Accuracy

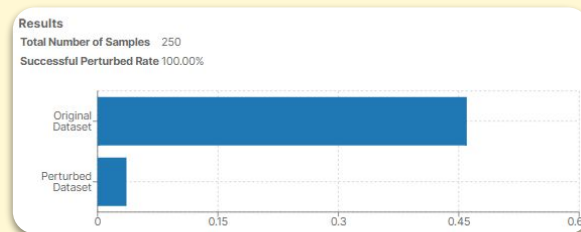
The measurement of fairness is based on a list of **metrics used to measure accuracy** including:

- False Negative Rate
- False Positive Rate
- False Discovery Rate
- False Omission Rate
- True Positive Rate
- True Negative Rate
- Positive Predictive Value
- Negative Predictive Value

Other metrics used to measure fairness includes:

- Equal Selection Parity
- Disparate Impact

AI Verify generate and display a bar chart of the original and perturbed dataset with interpretation of the results to **reflect the performance/accuracy of the AI model**.

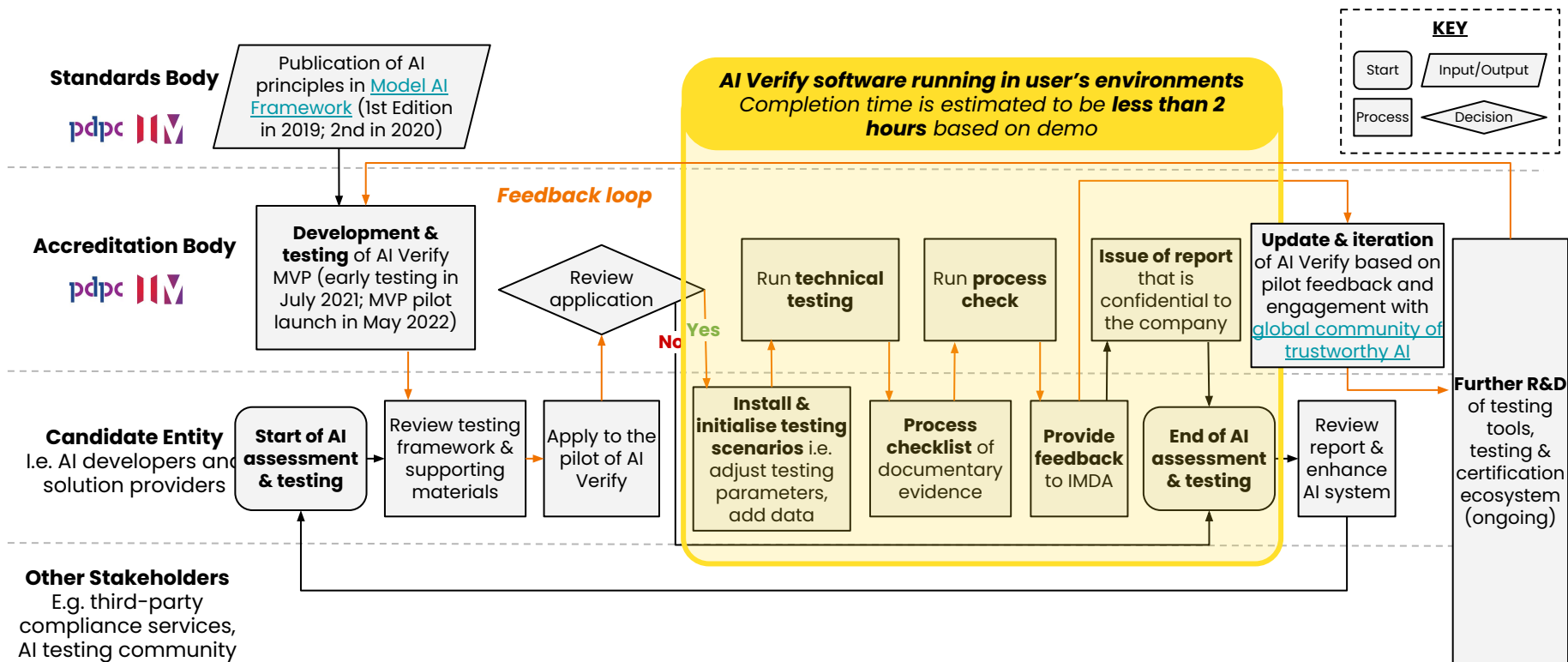


The longer the bar, the higher accuracy of the model.

02

AI
Verify

The pilot has embedded a feedback loop to collate industry best practice and feedback to inform iteration and further R&D



02

AI
Verify

Cross-sector collaboration plays a key role in building an AI accreditation ecosystem

RACI Matrix	Pre-Accreditation		Preparation		Assessment		Attestation	Post-Assessment		
	High-level principles set out	AI Verify development	Application	Creation of test scenario	Technical testing	Process checklist	Issue of report	Renewal of testing	Maintenance & feedback	Development of future certification scheme
Standards Body pdpc 	A R	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C
Accreditation Body pdpc 	N/A	A R	I	R	R	R	A R	R	A R	A R
Candidate Entity I.e. AI developers and solution providers	C	C	A R	A R	A R	A R	I	A R	C	C
Other Stakeholders E.g. third-party compliance services, AI testing community	C	C	N/A	N/A	C	N/A	N/A	N/A	C	R C

KEY

- A** Accountable: Those who are ultimately accountable for the correct and thorough completion of the deliverable or task
- R** Responsible: Those who do the work to achieve the task. There can be several R to perform one task
- C** Consulted: Those whose opinions are sought. Two-way communication
- I** Informed: Those who are kept up-to-date on progress, often only on completion of the task or deliverable. One-way communication
- N/A** Not Applicable: Those who are not involved in the task.

Source(s): [AI Governance Testing Framework and Toolkit: Invitation to Pilot](#), [Background on Singapore's AI Governance Work Overview](#), PUBLIC Analysis

02

AI
Verify

Singaporean regulators invested high technical effort upfront in developing automated testing tools to reduce ongoing burden

PUBLIC

Roles by Phase	Pre-Accreditation	Preparation	Assessment	Attestation	Post-Assessment
Standards Body 	International AI ethics; AI standardisation; Stakeholder engagement	N/A	N/A	N/A	AI standardisation; Stakeholder engagement
Accreditation Body 	Software engineering and development; User experience design	Expertise in AI testing	Software maintenance	Software maintenance	Expertise in AI testing; Software engineering Stakeholder engagement
Candidate Entity I.e. AI developers and solution providers	Technical expertise in AI (Ethical use of AI and data)	Software deployment; Application submission	Document uploading & data input	N/A	Technical expertise in AI (Ethical use of AI and data)
Other Stakeholders E.g. third-party compliance services, AI testing community	Technical expertise in AI (Ethical use of AI and data)	N/A	XYZ	N/A	Technical expertise in AI testing and certification; Accreditation schemes

KEY

High effort/resourcing

Medium effort/resourcing

Low effort/resourcing

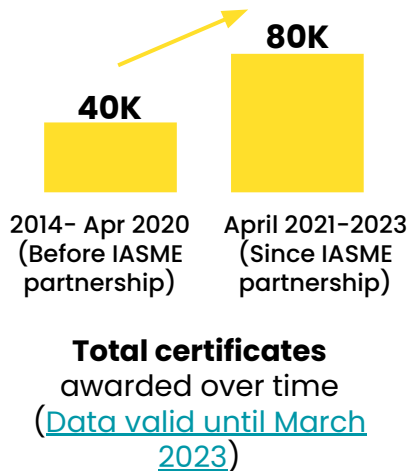
National Cyber Security Centre (NCSC)

Cyber Essentials Scheme

Cyber Essentials is a government-backed technical accreditation scheme with a third-party delivery partner

Partnering with **IASME Consortium**, the **National Cyber Security Centre (NCSC)** examines organisations' cyber risks through **independently verified self-assessment** (Cyber Essential, CE) and **additional technical audit** (Cyber Essential Plus, CE+), to **protect from most common cyber threats** and **demonstrate commitment** to cyber security

KEY STATS



CRITICAL SUCCESS FACTORS



Ongoing regular review

- **Regular review and evaluation** of the scheme ensures it keeps **evolving as the threat landscape and technology change**



High flexibility / accessibility

- **Two levels of certification** offer different levels of assurance, providing **flexibility** for organisations
- **Tiered pricing structure** ensures **accessibility** and **affordability** for businesses of all sizes.



Single pathway to accreditation

- **Singular delivery partner** via IASME
- **Clear and consistent pathway** for organisations to achieve CE/CE+ certification

LIMITATIONS

- The overall awareness of the scheme (14%) and adherence (5% for CE, 2% CE+) **remains low**. Med (8%) and large (12%) organisations indicated they adhere to standards, but **do not seek accreditation** whereas micro businesses indicated a **significant decrease** in reporting cybersecurity as a high priority (80% in 2022 to 68% 2023).
- Organisations bear **high burdens** of **annual renewal** which follows the same process as new accreditations.

***Note:** The CE/CE+ scheme was set up in 2014. The partnership with IASME Consortium as **the accreditation body** of CE/CE+ schemes has started since April 2020.
Source(s): [Cyber Essentials scheme: overview](#), [NCSC blog](#), [NCSC News: new look scheme protects businesses from cyber attack](#), [Review of Cyber Essentials influence on cyber security attitudes and behaviours in UK organisations](#), [Cyber security breaches survey 2023](#), PUBLIC Analysis

03

CE/CE+

A common 5 technical criteria are used for CE and CE+, incl. the use of firewalls, secure configuration management...

Organisations must demonstrate their compliance with **5 technical security controls (shown in this slide and next)** by completing a **self-assessment questionnaire** of binary choice, multiple choice, and text-based answers.

Technical Assessment Criteria for CE/CE+ (1 of 2)

#	Criteria	Metrics	Assessment Method
1	Firewalls: Use a firewall to secure internet connection	Organisations must protect every device in scope with a correctly configured firewall (or network device with firewall functionality). This includes: • Change default administrative passwords to a strong and unique password or disable remote administrative access entirely • Prevent access to the administrative interface from the internet • Block unauthenticated inbound connections by default • Ensure inbound firewall rules are approved and documented by an authorised person, and include The business need in the documentation • Remove or disable unnecessary firewall rules quickly, when they are no longer needed	• 12 questions • Multiple choice, binary choice and text-based description where necessary.
2	Secure configuration: Choose the most secure settings for devices and software	Organisations must proactively manage their computers and network devices. This includes regularly: • Remove and disable unnecessary user accounts • Change any default or guessable account passwords • Remove or disable unnecessary software • Disable any auto-run feature which allows file execution without user authorisation • Ensure users are authenticated before allowing them access to organisational data or services • Ensure appropriate device locking controls for users that are physically present	• 10 questions • Multiple choice, binary choice and text-based description where necessary.

...security update management, user access control, and malware protection

Technical Assessment Criteria for CE/CE+ (2 of 2)

#	Criteria	Metrics	Assessment Method
3	Security update management: Keep devices and software up to date	Organisations must make sure that all software in scope is kept up to date. All software on in-scope devices must: • Be licensed and supported • Removed from devices when it becomes unsupported or removed from scope by using a defined subset that prevents all traffic to / from the internet • Have automatic updates enabled where possible • Be updated, including applying any manual configuration changes required to make the update effective, within 14 days of an update being released	• 7 questions • Binary choice and text-based description where necessary
4	User access control: Control who has access to data and services	Organisations must be in control of their user accounts and the access privileges that allow access to their organisational data and services, and need to understand how user accounts authenticate and manage the authentication accordingly. This includes: • Have in place a process to create and approve user accounts • Authenticate users with unique credentials before granting access to applications or devices • Remove or disable user accounts when they're no longer required • Implement multi-factor authentication (MFA), where available • Use separate accounts to perform administrative activities only • Remove or disable special access privileges when no longer required	• 17 questions • Binary choice and text-based description where necessary
5	Malware protection: Protect from viruses and other malware	Organisations must make sure that a malware protection mechanism is active on all devices in scope.	• 5 questions • Multiple choice and binary choice.

03

To achieve CE+ certification, an additional technical auditing process is required by a licensed third-party

CE/CE+

Organisations must meet the requirements of **both CE and additional technical auditing** (i.e. passing all test case and sub-test) to achieve CE+ certification. Technical auditing is conducted by an independent, licensed IASME body.

Additional Technical Auditing for CE+

#	Test Case	Testing Method
1	Remote vulnerability assessment: Test whether an Internet-based opportunist attacker can hack into the Applicant's system with typical low-skill methods.	Vulnerability scanning. An external port scan of internet facing IP addresses will be conducted to ensure no clear and obvious misconfigurations or vulnerabilities can be identified.
2	Check patching by authenticated vulnerability scan of devices: Identify missing patches and security updates that leave vulnerabilities that threats within the scope of the scheme could easily exploit.	Representative sample testing. This test is performed on sampled end user devices (EUDs) that can connect to organisational data or services, servers and IaaS instances
3	Check malware protection: Check that all the devices in scope benefit from at least a basic level of malware protection	Representative sample testing. This test is performed on sampled sampled EUD, servers that provide a user-interactive desktop and IaaS instances.
4	Check Multi-factor authentication (MFA) configuration: Test cloud services declared in scope have been configured for MFA	Representative sample testing. This test is performed on all cloud services (IaaS, PaaS, or SaaS). All cloud services must be tested using a representative sample of user accounts. This must consist of at least one normal user and one administrative user for every cloud service used. The same users can be used across multiple cloud services.
5	Check account separation: Test user accounts don't have administrator privileges assigned.	Representative sample testing. This test is performed on sampled EUD, servers that provide a user-interactive desktop and cloud environments where administrative processes can run.

Source(s): [Cyber Essentials Plus: Illustrative Test Specification v3.1](#)

03

CE/CE+

IASME bodies conducting technical auditing must ensure the testing sample is representative of all devices in scope

*Representative sample testing is used for all computing devices including **end user devices (EUDs)**, **internally hosted servers**, and **all cloud services** (IaaS, PaaS, or SaaS).*

Additional Technical Auditing for CE+

For servers and EUDs

- The actual number of representative devices needed for test to achieve a satisfied level of confidence will **depend on the amount of variation** that exists as a result of the applicant's particular provisioning processes, and their effectiveness.
- Many organisations use standardised configurations for their servers and EUDs. In such cases, much of the organisation's equipment **can be covered by a small number of representative samples**.

For cloud services

- All cloud services must be tested using a representative sample of user accounts. This must **consist of at least one normal user and one administrative user for every cloud service used**. The same users can be used across multiple cloud services.

To obtain CE+ certification, applicants must pass every test case and sub-test of technical auditing

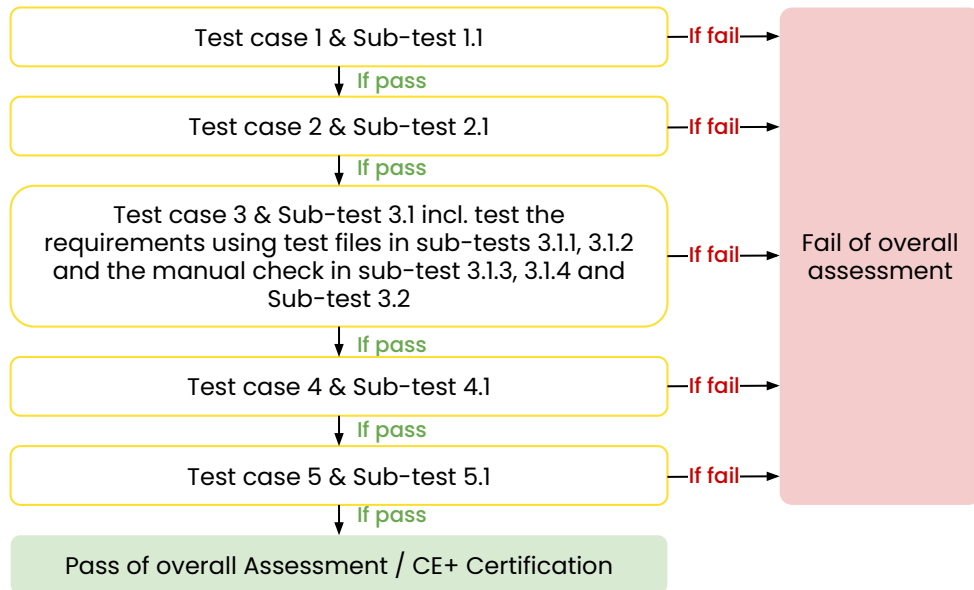
Additional Technical Auditing for CE+

Test Prerequisites

Prior to testing, **IASME licensed technical auditors must ensure** they:

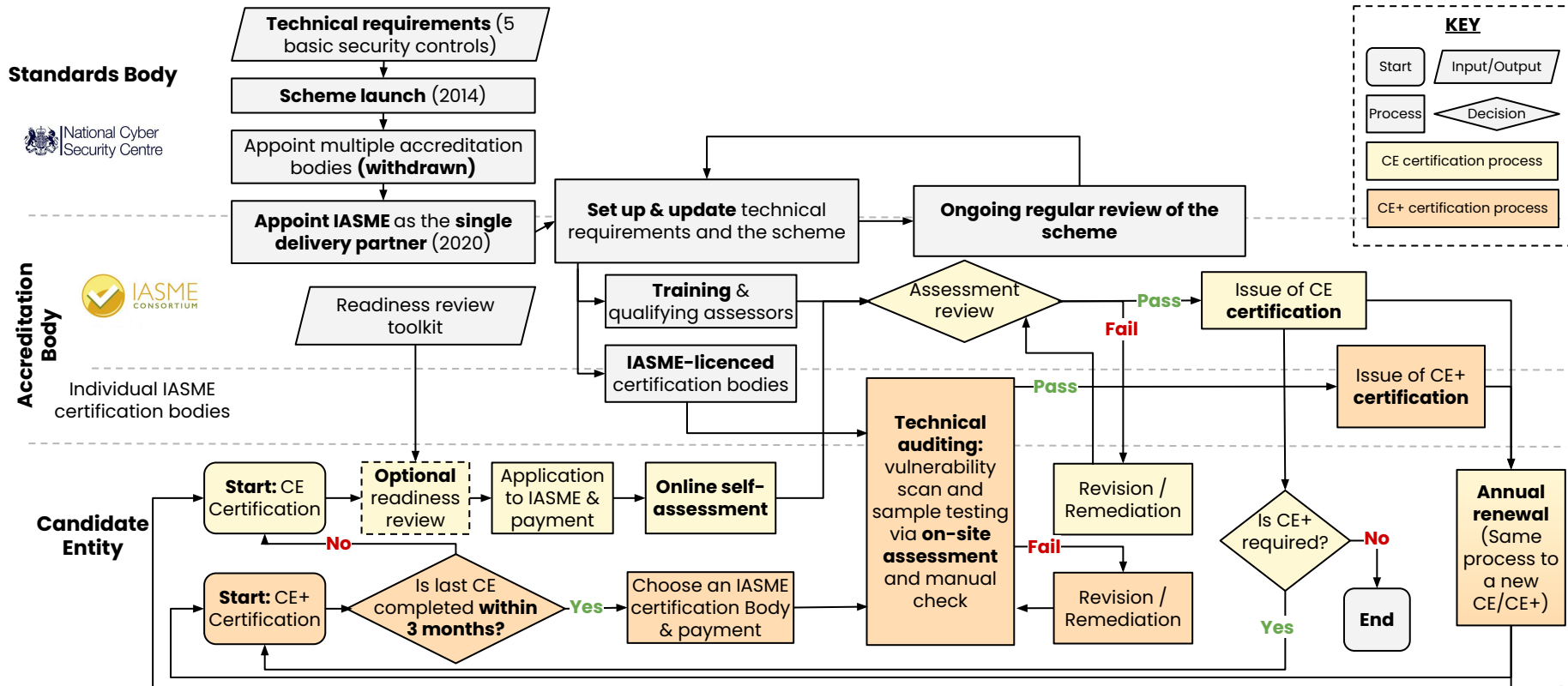
- Obtained the appropriate **written permission** from the applicant and **agreed the details and timing** of testing with the applicant;
- Have the **correct template** for the report;
- **Are able to** send arbitrary emails to an account operated by the applicant, test files, hosted on an external website owned by the certification body, access users with appropriate credentials to perform the tests, and working email clients and web browsers on a sample of the end user devices in scope.
- Have an **approved vulnerability scanning tool**
- Have **selected appropriate samples and sub-samples**

Test Results Interpretation



03 Due to its two-pronged approach, the Cyber Essentials forks into two processes - CE and CE+

CE/CE+



03

CE/CE+

NCSC leads the initiation, oversight and maintenance of the scheme and IASME is responsible for delivery and regular review

RACI Matrix		Pre-Accreditation		Preparation		Assessment		Attestation		Post-Assessment			
						CE		CE+					
		Technical requirements set out	Designation of accreditation body	Readiness review	Application	Self-assessment	Verification by qualified assessors	Technical auditing (incl. On-site assessment)	Feedback and Remediation	Issue of certification	Reapplication (if fail)	Renewal of certification	Technical requirements regular review & update
Standards Body		A	A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A
		R	R										R
Accreditation Body	 Individual IASME certification bodies	N/A	C	N/A	I (CE)	R	A	A	A	A	I (CE)	A	R
							R			R			
		N/A	N/A	N/A	I (CE+)	N/A	N/A	R	R	C	I (CE+)	R	I
Candidate Entity		N/A	N/A	A	A	A	N/A	R	R	I	A	R	N/A
				R	R	R					R		
KEY		A	R	C	I	N/A	Accountable: Those who are ultimately accountable for the correct and thorough completion of the deliverable or task Responsible: Those who do the work to achieve the task. There can be several R to perform one task Consulted: Those whose opinions are sought. Two-way communication Informed: Those who are kept up-to-date on progress, often only on completion of the task or deliverable. One-way communication Not Applicable: Those who are not involved in the task.						

Source(s): [IASME Cyber Essentials](#), [NCSC Cyber Essentials Resources](#), [Cyber Essentials technical requirements updated for April 2023](#), PUBLIC Analysis

03

CE/CE+

All parties need to have technical domain expertise and exert high/med effort for maintenance in response to evolving cyber threats

Roles by Phase	Pre-Accreditation	Preparation	Assessment		Attestation	Post-Assessment
			CE	CE+		
Standards Body  National Cyber Security Centre	Technical expertise in cybersecurity; Accreditation design; Compliance support	N/A	N/A	N/A	N/A	Expertise in cyber & evolving threats; Accreditation maintenance; Training
Accreditation Body  IASME CONSORTIUM Individual IASME certification bodies	Technical expertise; Accreditation design; Compliance support (e.g. readiness tool)	Training for assessors	Qualified assessor	Quality assurance	Quality assurance; Provision of reports and/or certificates	Technical expertise in cybersecurity; Accreditation maintenance; Training
	Technical expertise; Licensed by IASME	Assign technical auditor	N/A	Qualified auditor; Technical expertise	Technical expertise; Provision of assessment report	Training; Qualified auditor; Technical expertise
Candidate Entity	N/A	Eligibility and registration; Readiness review; Application fee	Technical expertise	Technical expertise	Technical expertise; Remediation effort;	Technical expertise; Reapplication / renewal fee & effort

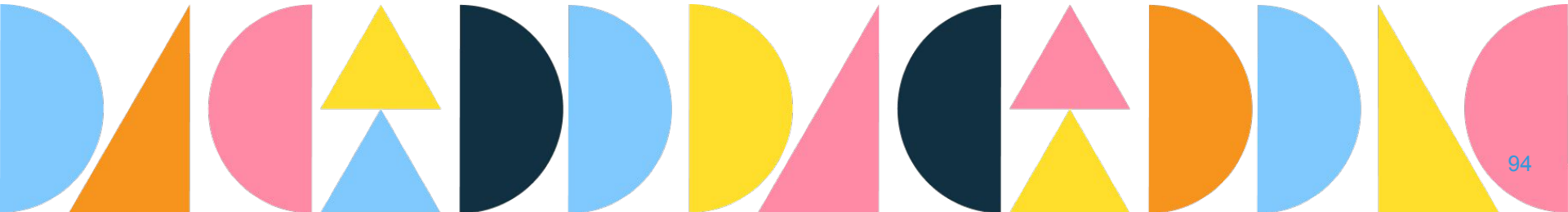
KEY

High effort/resourcing

Medium effort/resourcing

Low effort/resourcing

Conclusions



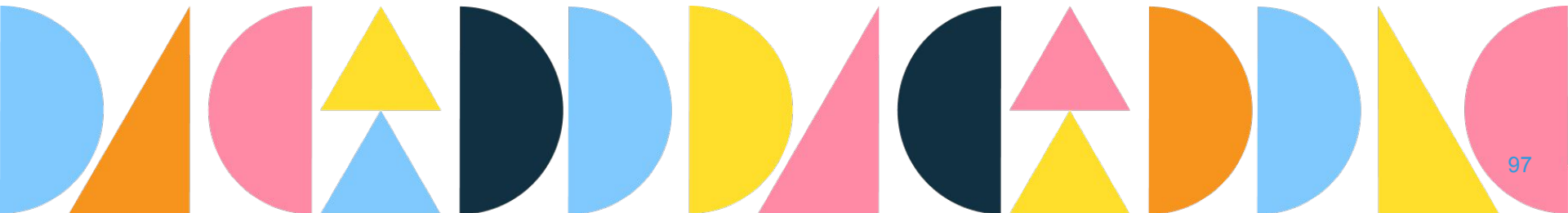
Conclusions

- To support Ofcom in its development of a robust **knowledge and evidence base on how technologies are evaluated and accredited**, **PUBLIC conducted research on accreditation approaches** used to ensure quality and consistency of products and services across various industries.
- Our research found that **the landscape of accreditation schemes is diverse, with a wide range of sectors and industries having their own unique accreditation systems**. These schemes often **cater to specific needs and challenges of each industry**, enabling organisations to meet specific standards and requirements.
- The effectiveness of the accreditation schemes we assessed **rely on characteristics that ensure they remain effective**. These centre primarily on their **adoption** (incentivising uptake, managing level of effort on parties involved), **continuous improvement** (adaptability to changing circumstances and facilitate scalability) and **structure** (type of approach, underlying principles and governance practices).
- In **fast-moving technology areas and innovative industries, the design of standards and accreditation processes is likely to be particularly challenging**. Many regulators and accreditation bodies have **chosen principles-based standards, and adaptable assessment** criteria in these areas, to ensure they remain relevant and effective.
- **Looking forward, cross-industry collaboration and harmonization among accreditation bodies** (nationally and internationally) is critical for **streamlining processes and minimising duplication of efforts**.

During our research we identified evidence gaps that were not publicly available or out of scope of this research project

Evidence Area	Evidence Gap	Future Mitigation
Process	Depending on the type of approach, accreditation bodies will request candidates to submit evidence and documentation. However, limited stakeholder engagement has prevented us to understand the barriers for accreditors in accessing such evidence and documentation from applicants and how that impacts the accreditation process .	• Stakeholder outreach to collect accreditation materials and interviews with accreditations bodies
Cost	There is very limited publicly available information around the exact costs for candidates that want to go through the accreditation process. This has limited our capacity to understand how the fees varies depending on applicants size and type of industry, how fees are calculated by accreditation bodies and the difference in cost between product and service.	• Stakeholder interviews with accreditations bodies
Effort	Given variances in level of review methods, evidence types and stakeholder engagement during application, the average time spent in applying and reviewing varies significantly per accreditation scheme. Exact determination of factors that impact time averages and variances cannot be determined without further engagement.	• Stakeholder interviews with accreditations bodies and user interviews with target applicants (ie. third-party tech providers)
Uptake	Accreditation bodies do not always publicly report the volume of drafted or completed applications , including the success and drop-out rates. Additionally, for those who engage with applicants and accredited bodies outside of the application process , they do not publicly share which events or resources incentivise and engage applicants.	• Stakeholder outreach to collect accreditation materials and user interviews with target applicants (ie. third-party tech providers)
Tech Landscape	To best inform Ofcom's accreditation scheme, it is key to understand the technical landscape across target users, including their solutions' technical archetypes, datasets, and more. Given the team did not conduct stakeholder interviews, there is a gap in understanding the barriers accreditors face in collecting and reviewing evidence , such as IP protection and sensitive data handling processes.	• Stakeholder interviews with accreditations bodies • User interviews with target applicants ('SafetyTech') • Tech landscape mapping through desk research • Tech horizon scanning to identify key potential barriers and changes

Appendix



Project definitions 1/2

PUBLIC

Concept	Definition	Sources
Accreditation	Accreditation refers to two scenarios: (1) the assessment of the conformity of products/services or providers of products/services with a set of criteria; (2) the assessment of the competence and impartiality of an organisation/individual that performs activities involved in (1). Please note that (1) does not necessarily require (2), but (2) can serve as a pre-accreditation step for scenario (1) when high levels of assurance are required.	PUBLIC definition: pulled from UKAS definition of certification and accreditation
Accreditation Body	The party that carries out the accreditation process.	Adapted from accreditation definition
Accreditation Process	We use accreditation process to refer to the process followed by all the involved parties to achieve the accreditation, assessment or certification	PUBLIC definition
Accreditation Scheme	We use accreditation scheme to refer to the specific systems for accrediting a technology or a service	PUBLIC definition
Certification	The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.	ISO Definition
Conformity Assessment	A process whereby a product, procedure, organisation, service or system is evaluated or measured against the relevant requirements. Such requirements are stated in standards, regulations, contracts, programmes, or other normative documents. Note, activities associated with conformity assessment include testing, inspection, certification, approval accreditation body, and quality assurance system registration.	A combination of the ISO definition , IEEE SA definition , & HMG definition
Conformity Assessment Body	The party that carries out the conformity assessment.	Adapted from conformity assessment definition

Project definitions 2/2

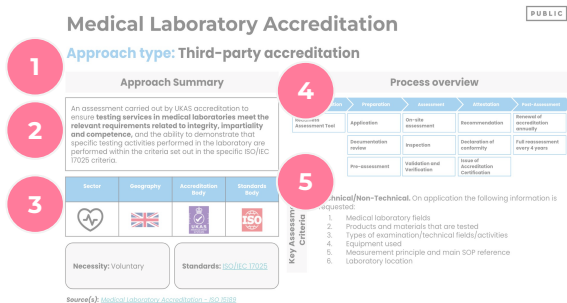
PUBLIC

Concept	Definition	Sources
Mixed approach Accreditation	Mix approach combines multiple accreditation approaches (e.g. verified self-assessment in combination with formal third-party accreditation, self-assessment overseen by a third party). This type of approach may or may not involve a third-party body serving as a formally approved accreditation body, an informal assessment body, or an oversight body, etc.	PUBLIC definition adapted from definitions of accreditation(s)
Principles-based approach to accreditation	Approach where the primary focus is on adherence with underlying principles that describe the objective of the accreditation scheme. A typical approach involves developing a framework with high-level principles set in legislation that in-scope organisations can adhere to.	PUBLIC based on Ofcom and MJA
Rules-based approach to accreditation	Approach where the primary focus is on compliance with a set of rules (i.e technical standards) in a prescriptive way. A typical approach involves developing (or adopting) a set of “standards”, and employing an auditing process to confirm that those standards have been met or not and the respective consequences.	PUBLIC based on Ofcom and MJA
Standardisation	Standardisation is the process of creating, issuing and implementing standards.	HMG definition
Standards	A standard is a document, commonly/often established by consensus and approved by a recognised body that provides rules, guidelines or characteristics for activities or their results. The aim is to achieve the greatest degree of order in a given context. Standards should provide a reliable basis for people to share the same expectations about a product or service.	PUBLIC & Ofcom definition adapted from HMG & BSI
Standardisation Body	The party that carries out the standardisation process to create, issue and implement standards.	Pulled from HMG's definition of standardisation
Third Party Accreditation	This type of accreditation is carried out by an approved third-party organisation assessing technology, product or service against certain requirements via testing, auditing and certification, etc. Third-party conducting assessment is typically appointed by regulators and qualified in line with relevant standards (i.e. ISO/IEC 17065).	PUBLIC definition adapted from UKAS and BSI

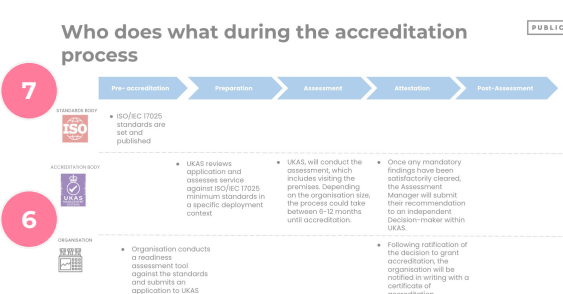
Accreditation Approaches Library: Reader Guide

PUBLIC

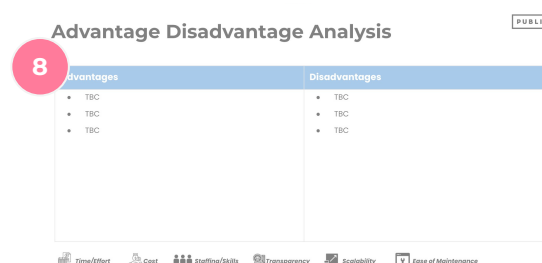
Page 1



Page 2



Page 3



1 **Type of approach:** Third party, self-accreditation or mixed approach

2 High-level overview of the approach

3 **Key information:** Sector, geography, accreditation body, standardisation body, applicable standard and whether the accreditation is voluntary or mandatory

4 Accreditation process diagram with main stages and activities

5 Assessment criteria the service or product is evaluated against (usually reflected in the respective standard)

6 Entities involved during the accreditation process

7 Stage of the process and key activity performed by each entity
(Note: to see more detailed information about the process please review long-list of approaches project document)

8 Advantages and disadvantages of each approach. Analysis based on desk research.

Accreditation Process: Reader Guide

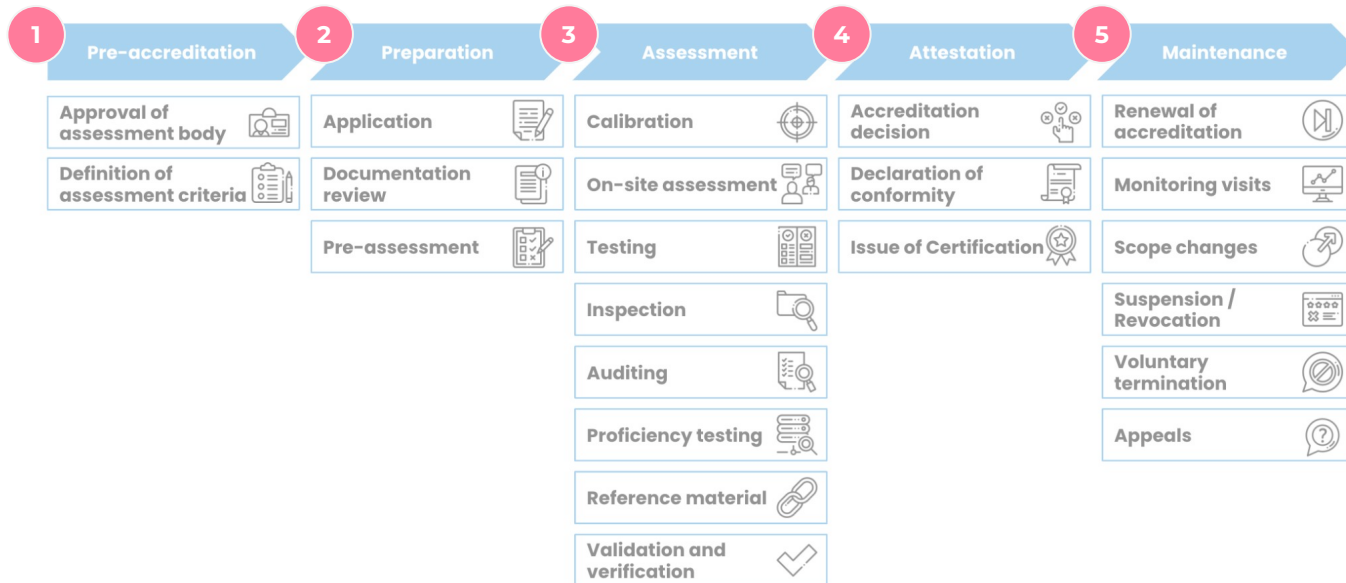
1 Pre-accreditation: Set up and launch of an accreditation scheme

2 Preparation: Activities involved to prepare for compliance

3 Assessment: Activities to assess the conformity to specified requirements

4 Attestation: Activities to convey the decisions and assurance

5 Maintenance: Ongoing assurance of compliance; Review and maintenance of the scheme



Bibliography (1/4)

Author	Sources
Alan Turing Institute	AI Standards Hub
BLab Global/BLab UK	How to certify as a B Corp - B Lab UK
BSI	Artificial Intelligence BSI
BSI	ISO 27001 - Information Security Management (ISMS) BSI
BSI	ISO/IEC 27017 - Security Controls for Cloud Services BSI
BSI	ISO/IEC 27018 - PII Protection in Public Clouds Certs BSI
BSI	ISO 31000 - Risk Management Certification - efficiency and governance BSI
CDEI	CDEI publishes research on AI governance - GOV.UK
CDEI	AI regulation: a pro-innovation approach - GOV.UK
DIN (Germany)	Artificial Intelligence Standardization helps create innovation- friendly framework conditions for the technol
DSIT	Growing the artificial intelligence industry in the UK - GOV.UK
EASA	Part-145 EASA
ENISA	NIS Directive — ENISA
EA	For Regulators - European Accreditation
European Commission	Policy and investment recommendations for trustworthy Artificial Intelligence Shaping Europe's digital future
FAA	Supplemental Type Certificates Federal Aviation Administration
FairTrade Foundation	Using the core FAIRTRADE Mark
FCA	Skilled person reviews FCA
ForHumanity	Independent Audit of AI Systems -
FSC	FSC UK
Hellios	JOSCAR : Hellios

Bibliography (2/4)

PUBLIC

Author	Sources
ICO	Measurement of Age Assurance Technologies ICO
ICO	Guidance on the AI auditing framework – Draft guidance for consultation ICO
ICO	Accountability and governance ICO
IEC	Understanding IEC 62443
IEEE SA	IEEE SA – IEEE 2089-2021
IEEE SA	7001-2021 – IEEE Standard for Transparency of Autonomous Systems
IEEE SA	IEEE Standard for Artificial Intelligence Exchange and Service Tie to All Test Environments (AI-ESTATE)
IEEE SA	IEEE – P7006 – Standard for Personal Data Artificial Intelligence (AI) Agent StandICT.eu 2026
IEEE SA	P7010/D1, Jun 2019 – IEEE Draft Standard for Well-being Metrics for Autonomous and Intelligent Systems
IEEE SA	7000-2021 – IEEE Standard Model Process for Addressing Ethical Concerns during System Design
IEEE SA	IEEE P7003TM Standard for Algorithmic Bias Considerations
IEEE SA	7007-2021 – IEEE Ontological Standard for Ethically Driven Robotics and Automation Systems
IEEE SA	IEEE SA – P7008
IEEE SA	IEEE SA – P7009
IEEE SA	IEEE SA – P7011
IEEE SA	IEEE SA – P7012
IEEE SA	P7013 Inclusion and Application Standards for Automated Facial Analysis Technology
IEEE SA	IEEE SA – The Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)
IMDA Singapore	Companion to the Model AI Governance Framework
ISO/IEC	ISO/IEC TR 24030:2021 – Information technology – Artificial intelligence (AI) – Use cases
ISO/IEC	ISO/IEC TR 24029-1:2021 – Artificial Intelligence (AI) – Assessment of the robustness of neural networks – Part 1: Overview

Bibliography (3/4)

Author	Sources
ISO/IEC	ISO/IEC 22989:2022 - Information technology – Artificial intelligence
ISO/IEC	ISO/IEC 23053:2022 - Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
ISO/IEC	ISO/IEC 38507:2022 - Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organizations
ISO/IEC	ISO/IEC 23894:2023 - Information technology – Artificial intelligence – Guidance on risk management
ISO/IEC	ISO/IEC TR 24028:2020 - Information technology – Artificial intelligence
ISO/IEC	ISO/IEC TR 24368:2022 - Information technology – Artificial intelligence – Overview of ethical and societal concerns
ISO/IEC	ISO/IEC TR 24027:2021 - Information technology – Artificial intelligence (AI) – Bias in AI systems and AI aided decision making
ISO/IEC	ISO/IEC TR 24372:2021 - Information technology – Artificial intelligence (AI) – Overview of computational approaches for AI systems
NCSC	About Cyber Essentials - NCSC.GOV.UK
NCSC	Cyber Assessment Framework - NCSC.GOV.UK
NCSC	All topics - NCSC.GOV.UK ion
NCSC	Supply chain security guidance - NCSC.GOV.UK
NCSC	Recovering a hacked account - NCSC.GOV.UK
NIST	Cybersecurity Framework NIST
NIST	Artificial intelligence NIST
NIST	NIST HANDBOOK 150
Ofcom	Online Safety Bill: Ofcom's roadmap to regulation
PDPC Singapore	PDPC Singapore's Approach to AI Governance
PDPC Singapore	DISCUSSION PAPER ON ARTIFICIAL INTELLIGENCE (AI) AND PERSONAL DATA – FOSTERING RESPONSIBLE DEVELOPMENT AND ADOPTION OF AI Pub

Bibliography (4/4)

PUBLIC

Author	Sources
Standards Australia	Metaverse risks & consumer safety requirements highlighted in new whitepaper – Standards Australia
Standards Australia	An Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard
TrustArc	TRUSTe Privacy Certification and Assurance Services
UKAS	Laboratory Accreditation – ISO/IEC 17025
UKAS	Medical Laboratory Accreditation – ISO 15189
UKAS	Point of Care Testing (POCT) Accreditation
UKAS	Quality Standard for Imaging (QSI) Accreditation
UKAS	Improving Quality in Physiological Services Accreditation (IQIPS)
UKAS	Medical Physics and Clinical Engineering Accreditation
UKAS	How to get UKAS Accreditation
UKAS	UKAS
UKAS	Health and Social Care Sector Accreditation UKAS
USGBC	LEED rating system U.S. Green Building Council