GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	**Name of Meeting** Quality, Safety and Improvement Committee **Date of Meeting** 25 Nov 2025 **Agenda item:** *4.2*

Policy / Procedure Approval Report

Section 1 - Policy / Procedure Information

Policy / Procedure Title	Clinical Audit Policy
Policy Lead	Jessica Taylor, Paula Mitchell
Lead Executive	Claire Birchall
PHW / All Wales?	PHW
Date of last Review	24 Oct 2025
Is the current policy / procedure within review date?	N/A – new policy
Approving Body /Group	Quality, Safety and Improvement Committee
Version Number	V1

Section 2: Recommendation
That the Quality, Safety and Improvement Committee: • **Considers** the information contained within the Clinical Audit Policy and Equalities Impact Assessment (Appendix 1) • **Note** that the Leadership Team endorsed the policy on 12.11.25 • **Approve** the policy as amended (Appendix1),

Section 3 – Details of the Review:	
Background:	
Reason for review	• N/A – this is a new policy
Description/Assessment	This is a new policy to set out the requirements for Public Health Wales to deliver its aims objectives, responsibilities and legal requirements transparently and consistently relating to clinical audit.
Consultation	
Has this Policy / Procedure been through the appropriate 28 day consultation process?	Yes
Date range of consultation:	25/09/25 – 23/10/25
Please provide details of any feedback received and outline what changes if any were made to the document as a result:	The policy was sent for consideration by current leads for clinical audit in the organisation in screening, health protection and infection services. All feedback received both written and verbal has been positive with no requests for changes.
Had this policy / procedure been considered by any other groups?	Leadership Team
If so, please provide detail of any comments / feedback or amendments made to the documents as a result of this	None

Section 4: Impact Assessments	
Equality and Health Impact Assessment	The EHIA is attached No significant impacts were identified
Welsh Language Impact	The Policy / Procedure will be translated to welsh and available on the internet bilingually.
Risk and Assurance	No implications
Health and Social Care (Quality and Engagement) (Wales) Act	The Duty of Quality (as part of the Health and Social Care (Quality and Engagement) (Wales) Act 2020) requires NHS bodies in Wales to conduct assessment of improvement in outcomes achieved through national clinical audit and internal audit programmes. Organisations are required to ensure they have systems and processes in place to provide assurance mechanisms in relation to

	clinical effectiveness and service delivery, of which clinical audit is key.
Financial implications	No implications
People implications	No implications
Socio Economic Duty	No implications

Section 5 - Implementation

Implementation plan (with timescales)		
Next steps	**Timescale**	**Responsible officer(s)**
Review of associated Quality and Clinical Procedure	By January 2026	Jessica Taylor

Section 6 – Dissemination

The primary source for dissemination of this policy within the organisation, wider community and our partners via the internet site.

Leads for clinical audit in clinical services in Public Health Wales will be informed when the policy is published.

GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	**Reference Number:** xxxx **Version Number:** xxx **Date of next review:** xxx

CLINICAL AUDIT POLICY

Policy Statement

This Policy sets out the necessary requirements for Public Health Wales (PHW) to deliver its aims, objectives, responsibilities and legal requirements transparently and consistently relating to clinical audit.

The Duty of Quality (as part of the Health and Social Care (Quality and Engagement) (Wales) Act 2020) requires NHS bodies in Wales to conduct assessment of improvement in outcomes achieved through national clinical audit and internal audit programmes (section 9.12). Organisations are required to ensure they have systems and processes in place to provide assurance mechanisms in relation to clinical effectiveness and service delivery, of which clinical audit is key (section 10.7).

We will develop and describe our "ways of working" in:

- Making national clinical audit data available to support publication of activity and outcome statistics
- Implement and/or respond to all relevant recommendations of any appropriate clinical audit
- Implement an ongoing, proportionate programme of clinical audit of our organisation's services in accordance with best practice
- Participate in national clinical audits within the National Clinical Audit and Patient Outcomes Programme (NCAPOP) relevant to Public Health Wales's services

The intended outcome of this policy is to support a culture of best practice in the management and delivery of clinical audit.

This policy aligns with the following strategic priorities:
- Delivering excellent public health services
- Supporting a sustainable health and care system

This policy is to be read in conjunction with PHW-STP06 Quality and Clinical Audit Procedure.

Policy Commitment

The intended outcome of this policy is to set out the rationale for clinical audit and provide a framework for such activity, including adherence to standards, guidance, and procedures.

Clinical audit is integral to improving quality, safety and service delivery in Wales. Audit provides an invaluable insight into the quality of services being provided and monitors how well improvements are being taken forward.

Public Health Wales uses clinical audit as an essential tool to drive quality improvement and provide quality assurance. Pivotal to this is directing comprehensive action towards areas of not meeting best practice standards. Quality is defined in the Duty of Quality as continuously, reliably, and sustainably meeting the needs of the population that we serve. In achieving this, NHS bodies will need to ensure that health services are safe, timely, effective, efficient, equitable and person-centred. These quality dimensions provide a framework to assess quality and guide improvement, and clinical audit is a key mechanism to achieve this.

PHW's Audit Team will provide oversight of the clinical audit programme and monitoring of the audit management system in compliance with this policy. The Audit Team will also provide support to staff to develop and design clinical audit projects.

This policy states the commitment of the organisation to ensure that all clinical services undertake a programme of clinical audit to provide assurance of clinical effectiveness and quality, and drive improvement.

This policy is intended to complement and not supersede existing guidance offered by professional bodies.

Supporting Procedures and Written Control Documents

All corporate policies and procedures are available on the Public Health Wales website

This policy will be support by the PHW-STP06 Quality and Clinical Audit Procedure, which describes the process for identifying, registering, undertaking and reporting clinical audits in PHW.

Both the policy and procedure are underpinned by The Duty of Quality, as part of the Health and Social Care (Quality and Engagement) (Wales) Act 2020.

Independencies with other policy/control documents:

1. Clinical Governance Framework
2. Information Governance
3. Risk Management Policy

Scope

This policy applies to anyone engaged in clinical audit processes within Public Health Wales, in all locations, including:

- All staff, including all levels of management, clinicians and non-clinicians and those on short term or honorary contracts
- Students and trainees in any discipline
- Participants, volunteers, patients and members of the public

This policy also applies when clinical audit is undertaken jointly across organisational boundaries.	
Impact Assessments	The impact assessments that have been completed for the Policy.
Approved by	Quality, Safety and Improvement Committee
Approval Date	TBC
Review Date	TBC
Date of Publication:	TBC
Group with authority to approve supporting procedures	PHW Leadership Team
Accountable Executive Director/Director	Claire Birchall, Executive Director of Nursing, Quality and Integrated Governance
Author	Quality and Clinical Governance Manager Quality and Clinical Audit Lead Head of Antenatal Screening Wales

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Board Business Unit.

This is a controlled document, the master copy is retained by the Board Business Unit

Whilst this document may be printed, the electronic version posted on the internet is the master copy. Any printed copies of this document are not controlled. This document should **not** be saved onto local or network drives but should always be accessed from the internet.

Summary of reviews/amendments				
Version number	**Date of Review**	**Date of Approval**	**Date published**	**Summary of Amendments**

Equality & Health Impact Assessment for Clinical Audit Policy

Please read the Guidance Notes in Appendix 1 prior to commencing this Assessment

Please note:

- The completed Equality & Health Impact Assessment (EHIA) must be
  - Included as an appendix with the cover report when the strategy, policy, plan, procedure and/or service change is submitted for approval
  - Published on the intranet and internet pages as part of the consultation (if applicable) and once agreed.
- Formal consultation must be undertaken, as required
- Appendices 1-3 must be deleted prior to submission for approval

Please answer all questions:-

1.	For service change, provide the title of the Project Outline Document or Business Case and Reference Number	Clinical Audit Policy
2.	Name of Corporate Directorate and title of lead member of staff, including contact details	Claire Birchall, Executive Director of Nursing, Quality and Integrated Governance
3.	Objectives of strategy/ policy/ plan/ procedure/ service	This Policy sets out the necessary requirements for Public Health Wales to deliver its aims, objectives, responsibilities and legal requirements transparently and consistently relating to clinical audit.
4.	Evidence and background information considered. For example	The Duty of Quality (as part of the Health and Social Care (Quality and Engagement) (Wales) Act 2020) requires NHS bodies in Wales to

	• population data • staff and service users data, as applicable • needs assessment • engagement and involvement findings • research • good practice guidelines • participant knowledge • list of stakeholders and how stakeholders have engaged in the development stages • comments from those involved in the designing and development stages Population pyramids are available from Public Health Wales Observatory and the 'Shaping Our Future Wellbeing' Strategy provides an overview of health need.	conduct assessment of improvement in outcomes achieved through national clinical audit and internal audit programmes (section 9.12). Organisations are required to ensure they have systems and processes in place to provide assurance mechanisms in relation to clinical effectiveness and service delivery, of which clinical audit is key (section 10.7). Clinical audit is integral to improving quality, safety and service delivery in Wales. Audit provides an invaluable insight into the quality of services being provided and monitors how well improvements are being taken forward.
5.	Who will be affected by the strategy/ policy/ plan/ procedure/ service	Clinical services, who are required under the Duty of Quality and the Clinical Governance Framework to have systems and processes in place to provide assurance mechanisms in relation to clinical effectiveness and service delivery. This policy strengthens this requirement.

6. EQIA / How will the strategy, policy, plan, procedure and/or service impact on people?

Questions in this section relate to the impact on people on the basis of their 'protected characteristics'. Specific alignment with the 7 goals of the Well-being of Future Generations (Wales) Act 2015 is included against the relevant sections.

How will the strategy, policy, plan, procedure and/or service impact on:-	**Potential positive and/or negative impacts**	**Recommendations for improvement/ mitigation**	**Action taken by Directorate / Division.** Make reference to where the mitigation is included in the document, as appropriate
6.1 Age For most purposes, the main categories are: • under 18; • between 18 and 65; and • over 65	Clinical Audit will not adversely impact upon this age range.	None required	
6.2 Persons with a disability as defined in the Equality Act 2010 Those with physical impairments, learning disability, sensory loss or impairment, mental health conditions, long-term medical conditions such as diabetes	The process for determining the choice of local clinical audit projects will not discriminate against any groups in society based on their disability and long term medical conditions. There is a potential positive impact if services undertake audits that can measure the equity of their services and	None required	

How will the strategy, policy, plan, procedure and/or service impact on:-	Potential positive and/or negative impacts	Recommendations for improvement/ mitigation	Action taken by Directorate / Division. Make reference to where the mitigation is included in the document, as appropriate
	therefore inform improvements in this area.		
6.3 People of different genders: Consider men, women, people undergoing gender reassignment **NB** Gender-reassignment is anyone who proposes to, starts, is going through or who has completed a process to change his or her gender with or without going through any medical procedures. Sometimes referred to as Trans or Transgender	The process for determining the choice of local clinical audit projects will not discriminate against any groups in society based on their gender reassignment. There is a potential positive impact if services undertake audits that can measure the equity of their services and therefore inform improvements in this area.	None required	
6.4 People who are married or who have a civil partner.	The process for determining the choice of local clinical audit projects will not discriminate against any groups in society based on marriage or civil partner reassignment, religion and	None required.	

How will the strategy, policy, plan, procedure and/or service impact on:-	Potential positive and/or negative impacts	Recommendations for improvement/ mitigation	Action taken by Directorate / Division. Make reference to where the mitigation is included in the document, as appropriate
	belief		
6.5 Women who are expecting a baby, who are on a break from work after having a baby, or who are breastfeeding. They are protected for 26 weeks after having a baby whether or not they are on maternity leave.	The process for determining the choice of local clinical audit projects will not discriminate against any women in society.	None required	
6.6 People of a different race, nationality, colour, culture or ethnic origin including non-English speakers, gypsies/travellers, migrant workers	The process for determining the choice of local clinical audit projects will not discriminate against any groups in society based on their race, sex, age, sexual orientation, religion and belief. There is a potential positive impact if services undertake audit that can measure the equity of their services and	None required	

How will the strategy, policy, plan, procedure and/or service impact on:-	Potential positive and/or negative impacts	Recommendations for improvement/ mitigation	Action taken by Directorate / Division. Make reference to where the mitigation is included in the document, as appropriate
	therefore inform improvements in this area.		
6.7 People with a religion or belief or with no religion or belief. The term 'religion' includes a religious or philosophical belief	The process for determining the choice of local clinical audit projects will not discriminate against any groups in society based on religion and belief	None required	
6.8 People who are attracted to other people of: • the opposite sex (heterosexual); • the same sex (lesbian or gay); • both sexes (bisexual)	The process for determining the choice of local clinical audit projects will not discriminate against any groups in society based on their sexual orientation	None required	
6.9 People who communicate using the Welsh language in terms of correspondence, information leaflets, or service plans and design Well-being Goal – A Wales of vibrant culture and	The process for determining the choice of local clinical audit projects will not discriminate against any groups in society based on the Welsh Language. There is a potential positive impact if services undertake	None required	

How will the strategy, policy, plan, procedure and/or service impact on:-	Potential positive and/or negative impacts	Recommendations for improvement/ mitigation	Action taken by Directorate / Division. Make reference to where the mitigation is included in the document, as appropriate
thriving Welsh language	audit that can measure the equity of their services and therefore inform improvements in this area.		
6.10 People according to their income related group: Consider people on low income, economically inactive, unemployed/workless, people who are unable to work due to ill-health	The process for determining the choice of local clinical audit and or service evaluation projects will not discriminate against any groups in society based on their economic status	None required	
6.11 People according to where they live: Consider people living in areas known to exhibit poor economic and/or health indicators, people unable to access services and facilities	The process for determining the choice of local clinical audit projects will not discriminate against any groups in society based on economic status. There is a potential positive impact if services undertake audit that can measure the equity of their services and therefore inform	None required	

How will the strategy, policy, plan, procedure and/or service impact on:-	Potential positive and/or negative impacts	Recommendations for improvement/ mitigation	Action taken by Directorate / Division. Make reference to where the mitigation is included in the document, as appropriate
	improvements in this area.		
6.12 Consider any other groups and risk factors relevant to this strategy, policy, plan, procedure and/or service	No other risks identified	None	

7. HIA / How will the strategy, policy, plan, procedure and/or service impact on the health and well-being of our population and help address inequalities in health?

Questions in this section relate to the impact on the overall health of individual people and on the impact on our population. Specific alignment with the 7 goals of the Well-being of Future Generations (Wales) Act 2015 is included against the relevant sections.

How will the strategy, policy, plan, procedure and/or service impact on:-	**Potential positive and/or negative impacts and any particular groups affected**	**Recommendations for improvement/ mitigation**	**Action taken by Directorate / Division** Make reference to where the mitigation is included in the document, as appropriate
7.1 People being able to access the service offered: Consider access for those living in areas of deprivation and/or those experiencing health inequalities Well-being Goal - A more equal Wales	The process for determining the choice of local clinical audit projects will not impact on people being able to access services. There is a potential positive impact if services undertake audit that can measure the equity of their services and therefore inform improvements in this area.	None required	
7.2 People being able to improve /maintain healthy lifestyles: Consider the impact on healthy lifestyles, including healthy eating, being active, no smoking /smoking cessation, reducing the	The process for determining the choice of local clinical audit projects will not impact on people's healthy lifestyles.	None required	

How will the strategy, policy, plan, procedure and/or service impact on:-	Potential positive and/or negative impacts and any particular groups affected	Recommendations for improvement/ mitigation	Action taken by Directorate / Division Make reference to where the mitigation is included in the document, as appropriate
harm caused by alcohol and /or non-prescribed drugs plus access to services that support disease prevention (eg immunisation and vaccination, falls prevention). Also consider impact on access to supportive services including smoking cessation services, weight management services etc Well-being Goal – A healthier Wales			
7.3 People in terms of their income and employment status: Consider the impact on the availability and accessibility of work, paid/ unpaid employment, wage levels, job security, working conditions	The process for determining the choice of local clinical audit projects will not impact people in terms of their income or employment	None required	

How will the strategy, policy, plan, procedure and/or service impact on:-	Potential positive and/or negative impacts and any particular groups affected	Recommendations for improvement/ mitigation	Action taken by Directorate / Division Make reference to where the mitigation is included in the document, as appropriate
Well-being Goal – A prosperous Wales			
7.4 People in terms of their use of the physical environment: Consider the impact on the availability and accessibility of transport, healthy food, leisure activities, green spaces; of the design of the built environment on the physical and mental health of patients, staff and visitors; on air quality, exposure to pollutants; safety of neighbourhoods, exposure to crime; road safety and preventing injuries/accidents; quality and safety of play areas and open spaces Well-being Goal – A resilient Wales	The process for determining the choice of local clinical audit projects will not impact people in terms of their physical environment	None required	

How will the strategy, policy, plan, procedure and/or service impact on:-	Potential positive and/or negative impacts and any particular groups affected	Recommendations for improvement/ mitigation	Action taken by Directorate / Division Make reference to where the mitigation is included in the document, as appropriate
7.5 People in terms of social and community influences on their health: Consider the impact on family organisation and roles; social support and social networks; neighbourliness and sense of belonging; social isolation; peer pressure; community identity; cultural and spiritual ethos Well-being Goal – A Wales of cohesive communities	The process for determining the choice of local clinical audit projects will not impact social and community influences on health	None required	
7.6 People in terms of macro-economic, environmental and sustainability factors: Consider the impact of government policies; gross domestic product; economic development; biological diversity; climate	The process for determining the choice of local clinical audit projects will not impact macro-economic, environmental and sustainability factors	None required	

How will the strategy, policy, plan, procedure and/or service impact on:-	Potential positive and/or negative impacts and any particular groups affected	Recommendations for improvement/ mitigation	Action taken by Directorate / Division Make reference to where the mitigation is included in the document, as appropriate
Well-being Goal – A globally responsible Wales			

Please answer question 8.1 following the completion of the EHIA and complete the action plan

8.1 Please summarise the potential positive and/or negative impacts of the strategy, policy, plan or service	No negative impacts of this policy were identified. There is a potential for positive impact, should services choose to audit areas where quality of equity is measured and acted upon.

Action Plan for Mitigation / Improvement and Implementation

	Action	Lead	Timescale	Action taken by Directorate / Division
8.2 What are the key actions identified as a result of completing the EHIA?	None required.			

	Action	Lead	Timescale	Action taken by Directorate / Division
8.3 Is a more comprehensive Equalities Impact Assessment or Health Impact Assessment required? This means thinking about relevance and proportionality to the Equality Act and asking: is the impact significant enough that a more formal and full consultation is required?	No			

	Action	Lead	Timescale	Action taken by Directorate / Division
8.4 What are the next steps? Some suggestions:- • Decide whether the strategy policy, plan, procedure and/ service proposal: ○ continues unchanged as there are no significant negative impacts ○ adjusts to account for the negative impacts ○ continues despite potential for adverse impact or missed opportunities to advance equality (set out the justifications for doing so) ○ stops. • Have your strategy, policy, plan, procedure and/or service proposal approved • Publish your report of this impact assessment • Monitor and review	The policy continues unchanged as there are no significant negative impacts.			

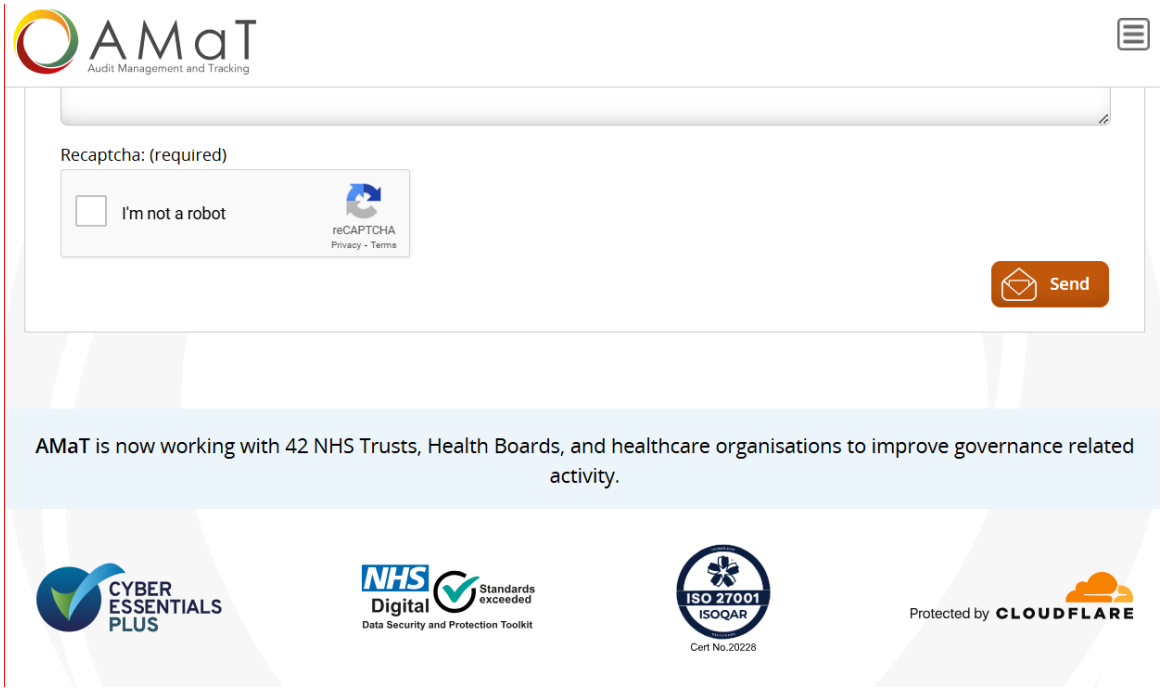
Request for approval of processing

Information Asset ref no:	
Information Asset title:	**Audit Management and Tracking Tool (AMaT)**
Information Asset Owner:	**Angela Cook Assistant Director of Nursing & Quality**

Please enter details of processing requested below

AMaT is a web-based system for the oversight, management and tracking of audit and quality improvement activity, allowing real time data input via smartphone, tablet, or desktop computer. It has a number of modules contained within the system. No Personal identifiable information (PII) will be held on the system as audit and Quality Improvement (QI) should always be anonymised. Public Health Wales (PHW) Staff will be trained to use the system as part of its implementation with ongoing access to support. Organisational hierarchy will be required to support use of the tools with the AMaT system. The only information provided for this will be staff emails and potentially workplace location.

The company has the following accreditation:
Cyber essentials in date until Feb 25 – company are renewing this.
ISO 27001 in date until 8 Nov 27.



Discussed with Information Governance (IG) (Lisa Partridge) on 22 Nov 24 – guidance given is that data processing agreement will only be required, not full DPIA. Further discussion on 19 Dec 24 with Lisa Partrdige has highlighted that as this system is being procured through Shared Services G Cloud Framework: information available here Microsoft Word - DRAFT AMaT Service Definition Document v1.3.docx – page 9 specifically refers to data.

Extract:
All data on AMaT is held within secure data centres in the UK that comply with ISO 27001 security standards and protected by Cloudflare. Full backups are taken daily by both the hosting company and Meantime IT Ltd (the company that develops AMaT).
Disaster recovery and business continuity processes are covered by the ISO 27001 accreditations of both Meantime IT Ltd and Meantime AMaT Ltd, which are audited annually by a third party, ISOQAR. Any issue at the data centre, where information is stored, is mitigated by instant failover to a separate data centre.
The organisation licensing AMaT (and MaMR) is the data controller. Meantime AMaT Ltd is the data processor. It is the data controller's responsibility to ensure that the data held within their instance of AMaT meets their organisation's information governance requirements.

The modules within AMaT are:

- Clinical/ Ward Audit – these modules provide full oversight and management of audit activity across the organisation. No PII will be held for audit activity, Any patient data will be anonymised.
- Guidance – NICE guidance/ Standard Operating Procedures (SOPS) and other key guidance documents will be uploaded here.
- Inspections – Inspection reports will be uploaded into this area. Names of those undertaking inspections will be visible.
- Morbidity and mortality module – PHW will not be using this module.
- Quality Improvement – no PII should be contained in this module.

Data Protection Impact Assessment (DPIA2) Required ~~Yes~~ / No*

Please enter rationale for the decision below

Data Protection Officer advice sought? Yes / ~~No~~*

If yes, IG Service to complete with advice

Yes initially Lisa Partridge.

Processing approved Yes / ~~No~~	
Signed (IAO)	**Angela Cook**
Date	**13.12.2024**
Date of next review	**30.6.2025**

***** **Delete as appropriate**

Cyber Security Requirements for systems hosted in the cloud.

Introduction

This document provides the Cyber Security requirements for Cloud hosted systems procured by Public Health Wales. Cloud hosted systems are defined as systems developed, managed or hosted external to Public Health Wales & NHS Wales.

Public Health Wales will hereon be referred to as the Authority and the bidder hereon referred to as the Contractor.

Guidance for bidders

Bidders are to review each numbered requirement and to respond to each. The response must provide an indication of the bidder's level of compliance (see table below) as well as a detailed description of their capabilities in each area and any supporting evidence.

The Authority understands the nature of the ever-evolving threat landscape and would ask that bidders be honest in their response so that a pragmatic approach to scoring can take place; we recognise that not all requirements will be satisfied and that a proportionate approach to risk is needed.

For each requirement, state your current compliance status and provide the necessary evidence as described in the table below.

Level of Compliance	**Description**
Fully compliant	The Contractor's system fully satisfies the requirement (listed in the description). Evidence will be provided to demonstrate the current capabilities of the Contractor's system.
Working towards compliance	The Contractor's system partially meets the requirement and there are plans to develop the system to achieve full compliance. Evidence will be provided to show the road map of future releases of when the missing functionality will be introduced.
Partially compliant	The Contractor's system partially meets the requirement and there are no plans to develop the system to achieve full compliance. Evidence will be provided to show the current functionality which satisfies the requirement.
Not compliant	The Contractor's system does not meet the requirement. No evidence is required.

Cyber Security Principles

Reference	Description
CYB_CSP_11.	The Contractor acknowledges that the Authority places great emphasis on maintaining the Confidentiality, Integrity and Availability of the Contractor System. This applies to all aspects, including Infrastructure, Systems, Services, Information and its interaction with other Authority services.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Meantime AMaT Ltd is ISO 27001 certified, CE+ certified, and DSP toolkit certified. In addition, the company's employees undergo annual GDPR training and there are monthly ISM meetings.
CYB_CSP_22.	The Contractor shall be responsible for the security of the Contractor System and must always provide a level of security which is in accordance with security industry Good Practice and UK / EEA Data Protection Legislation.
Level of Compliance	**Supplier supporting statement**
Fully compliant	AMaT is a cloud-based system entirely managed by Meantime AMaT. The security processes and procedures are certified under ISO 27001 and all security patches are applied in a timely manner.
CYB_CSP_33.	The Contractor must commit to continual improvement of the controls within Contractor System in line with the changing threat landscape and the availability of new/improvement controls.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 policies and procedures.
CYB_CSP_44.	The Contractor will ensure that Cyber Security considerations are made at all stages of the life cycle and that the principles of Secure By Design are followed in all iterations of development of the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Meantime AMaT is ISO 27001 certified, and our software development life cycle is covered in document A14 as per our statement of applicability.
CYB_CSP_55.	The Contractor will implement the principle of Defence In Depth and will ensure that protection is provided not just a single layer of protection, but will be through a combination of measures distributed logically.
Level of Compliance	**Supplier supporting statement**

Reference	Description
Fully compliant	AMaT is protected by Cloudflare WAF. All data transmission is across HTTPS / TLS 1.3. We operate on a high availability Microsoft Azure server with geo-redundant failover. Access to AMaT is by username and password or single sign on. All data is encrypted at rest (AES 256).

Compliance

Reference	Description
CYB_COM_66.	The Contractor should hold the ISO/IEC 27001 accreditation or Cyber Essentials plus (CE+).
Level of Compliance	**Supplier supporting statement**
Fully compliant	Meantime AMaT holds both ISO 27001 and CE+ certification.
CYB_COM_77.	The certification(s) must be provided by a suitable certification body which are recognised by the United Kingdom Accreditation Service (https://www.ukas.com/) or the IAF (https://iaf.nu/en/home/)https://iaf.nu/en/home/
Level of Compliance	**Supplier supporting statement**
Fully compliant	ISO 27001 certification is provided by Alcumus ISOQAR. CE+ certification is provided by IASME consortium.
CYB_COM_88.	The Contractor recognises that they must maintain a current and valid certification during the contract.
Level of Compliance	**Supplier supporting statement**
Fully compliant	All of Meantime AMaT's security certification is renewed at the appropriate intervals.
CYB_COM_99.	The scope of the accreditation must include all aspects of the organisation that are involved in the provision of the managed service.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Meantime AMaT's ISO 27001 public statement of applicability has been provided with this document.
CYB_COM_1010.	The Contractor must provide a copy of their Statement of Applicability for review by the authority. Attention must be drawn to any exemptions which will be reviewed and require mutual agreement as to the reason for exemption.
Level of Compliance	**Supplier supporting statement**

Reference	Description
Fully compliant	Meantime AMaT's ISO 27001 public statement of applicability has been provided with this document

Data in transit protection

Reference	Description
CYB_DIT _1111.	The Contractor must ensure that all data transiting the Contractor System is adequately protected (i.e. TLS 1.2) against tampering and eavesdropping. This will apply to all data, specifically: • Data transit between end user device(s) and the service • Data in transit as it flows between internal components within the service • Data that is exposed to other external services, such as via an API
Level of Compliance	**Supplier supporting statement**
Fully compliant	Data is encrypted at rest (AES256) and transmitted over HTTPS / TLS 1.3, including for APIs.
CYB_ DIT _1212.	The Contractor will ensure that any bulk data upload and/or onboarding of data will have the same level of protection as in life data flows.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Data is transmitted over HTTPS / TLS 1.3 in all instances.
CYB_ DIT _1313.	The Contractor must maintain a list of all external data flows used within the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	N/A
CYB_ DIT _1414.	The Contractor must provide assurances that all internal data flows within the Contractor System are adequately protected. This includes when data is moved between physical sites and availability zones.
Level of Compliance	**Supplier supporting statement**
Fully compliant	All internal data flows are HTTPS / TLS 1.3. No data is moved between physical sites and availability zones.
CYB_ DIT _1515.	The Contractor will be responsible for the management of encryption keys and certificates which are used to protect data.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This process is covered by Meantime AMaT's ISO 27001 statement of applicability.

Reference	Description
CYB_ DIT _1616.	The lifetime of certificates will be proportional to the sensitivity of the data it is used to protect.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This process is covered by Meantime AMaT's ISO 27001 statement of applicability.

Asset protection and resilience

Reference	Description
Physical location and legal jurisdiction	
CYB_APR_1717.	The Contractor must ensure that all data stored and/or processed as part of the Contractor System will be handled within the UK / EEA legislation applicable to the data being used. The transiting Contractor System is adequately protected against tampering and eavesdropping.
Level of Compliance	**Supplier supporting statement**
Fully compliant	AMaT and its data is hosted on Microsoft Azure with document storage on Amazon S3. All servers are based in the UK and protected by Cloudflare WAF.
CYB_ APR _1818.	Should there be any change to the location of the storage and/or processing of data during the term of the contract, then the Contractor will inform the Authority.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Meantime AMaT regularly communicates any change in service to the Super User Group which is formed from representatives of each licensed organisation.
CYB_ APR _1919.	As a Data Processor, the Contractor will store and/or process data on behalf of the Authority who will remain the Data Controller.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed.
Data centre security	
CYB_ APR _2020.	The Contractor will ensure that the physical storage of data is within a tier II (or higher) data centre.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. AMaT and its data is hosted on Microsoft Azure with document storage on Amazon S3.
Data encryption	
CYB_ APR _2121.	The Contractor will ensure that all data at rest is protected by encryption.

Reference	Description
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. All data is protected at rest by AES256
CYB_ APR _2222.	The encryption standards used for protection of data at rest will be the same strength as those used for the protection of data in transit
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. All data is protected at rest by AES256 and transmitted using HTTPS / TLS1.3
Backups	
CYB_ APR _2323.	The Contractor will ensure that all data and configuration items within the Contractor System will be subjected to a backup routine and will be stored within an immutable backup solution
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. Additionally, Microsoft Azure allows real-time fail-over, on datacentres in the UK.
Data sanitisation and equipment disposal	
CYB_ APR _2424.	The Contractor will ensure that all data is erased when resources are moved or re-provisioned
Level of Compliance	**Supplier supporting statement**
Fully compliant	This is covered by Meantime AMaT's ISO 27001 policies and also by Microsoft's.
CYB_ APR _2525.	In the case that dedicated hardware is used to store/process data, then the hardware must undergo secure disposal at the of the life decommissioning process
Level of Compliance	**Supplier supporting statement**
Fully compliant	AMaT is a cloud-based system. Hardware destruction is the responsibility of Microsoft.

Separation between customers

Reference	Description
CYB_SBC_2626.	The Contractor will ensure that there are robust controls in place to ensure separation of the data stored/processed within the Contractor System and other systems hosted on any shared infrastructure
Level of Compliance	**Supplier supporting statement**
Fully compliant	Separation of data is done logically at database level as this is SaaS. All system data can be traversed up to its originating organisation record. When a user logs in, the organisation ID is found based on

Reference	Description
	their account and then the system data views are built using that predicate. The system will not render without that predicate. Pages incorporate checks to ensure a user is viewing data they are authorised to view and that includes (but is not limited to) data that belongs to the user's organisation only. The infrastructure is exclusive to AMaT, and not shared by any other systems.

Governance framework

Reference	Description
CYB_GF_2727.	The Contractor must have a robust governance structure in place, which has responsibility for Security of the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Meantime AMaT is ISO 27001 and CE+ certified.
CYB_GF_2828.	The Contractor must have a nominated senior management representative with responsibility for the risks associated with the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Meantime AMaT is ISO 27001 and CE+ certified.

Operational security

Reference	Description
Vulnerability management	
CYB_OS_2929.	The Contractor will implement a technical vulnerability management solution which will assess the Contractor Service on a regular basis and will identity known or suspected vulnerabilities.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Meantime AMaT is partnered with NCSC who do a daily light PEN test against top threats. Additional unit PEN tests are carried out on the AMaT / Meantime framework. We can accommodate one off tests at trust requests.
CYB_OS_3030.	The vulnerability management solution will be deployed across all Components within the Contractor Service and will be kept continually up to date.
Level of Compliance	**Supplier supporting statement**

Reference	Description
Fully compliant	Confirmed.
CYB_OS_3131.	The Contractor will review all identified vulnerabilities and take any necessary action, depending on the level of risk presented to the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. This forms part of Meantime AMaT's ISO 27001 policies and procedures.
CYB_OS_3232.	The Contractor will implement a patching schedule and will apply it to all components it has responsibility for.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Within 14 days of any software update being made available (critical or otherwise) we: 1. Install the updates on all non-production servers immediately 2. Ensure that the updates do not affect availability or integrity of data to the non-production servers 3. Assuming there are no issues we then install them immediately on the production servers 4. All servers are automatically rebooted on a 14 day cycle on Sunday evenings outside of office hours 5. Any updates that require a full reboot to be 100% effective are thus always applied within 14 days
CYB_OS_3333.	Patches which meet one or more of the following criteria, will be applied immediately upon being made available by the manufacturer: • A vulnerability, the exploitation of which could allow code execution without user interaction. These scenarios include self-propagating malware (e.g. network worms), or unavoidable common use scenarios where code execution occurs without warnings or prompts, such as can occur during browsing to a web page or opening email; • A vulnerability, the exploitation of which could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of the Services. These scenarios include common use scenarios where client is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability. Sequences of user actions that do not generate prompts or warnings are also covered; • The vulnerability is high risk and requires little or moderate levels of specialized knowledge to exploit;

Reference	Description
	• Security updates classified as Critical, Severe, High Important, High risk or similar.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed as per Meantime AMaT's ISO 27001 statement of applicability.
CYB_OS_3434.	All other patches will be applied within 1 month of manufacture release.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Within 14 days of any software update being made available (critical or otherwise) we: 1. Install the updates on all non-production servers immediately 2. Ensure that the updates do not affect availability or integrity of data to the non-production servers 3. Assuming there are no issues we then install them immediately on the production servers 4. All servers are automatically rebooted on a 14 day cycle on Sunday evenings outside of office hours 5. Any updates that require a full reboot to be 100% effective are thus always applied within 14 days
CYB_OS_3535.	The Contractor will ensure that the availability of the Services is not compromised during the patching process and technical / procedural processes are implemented to maintain the availability of the Services
Level of Compliance	**Supplier supporting statement**
Fully compliant	Holding pages are used whilst the system is updated to ensure there are no data integrity issues.
Malware Protection	
CYB_OS_3636.	The Contractor will implement a technical solution, capable of preventing, detecting and repairing from malware and malicious code across all Components within the Contractor System and will ensure that the solution is kept continually up to date with signatures and IoC's.
Level of Compliance	**Supplier supporting statement**
Fully compliant	AMaT is a cloud-based system protected by Cloudflare and Microsoft Defender.
Pen testing	
CYB_OS_37.	The Contractor will commission a penetration test assessment of the Services prior to go-live, after any significant infrastructure/system changes, and at least once per year.
Level of Compliance	**Supplier supporting statement**

Reference	Description
Fully compliant	Meantime AMaT is partnered with NCSC who do a daily light PEN test against top threats. Additional unit PEN tests are carried out on the AMaT / Meantime framework. We can accommodate one off tests at trust requests. Please note, AMaT has been live since 2016 and the onboarding of new organisations is not treated as a 'go live' situation.
CYB_OS_38.	The Penetration testing will be based on industry-accepted penetration testing approaches (i.e. CHECK). As a minimum, it will test the following areas: • Infrastructure • Application • Client access (Mobile and/or desktop) • Data transfers
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed.
CYB_OS_39.	The scope of the penetration testing will be provided to the Authority for review, and approval, prior to commissioning the testing.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed.
CYB_OS_40.	The full report providing the results the penetration testing will be provided to the Authority, immediately to review.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Some of our Trusts register with the NCSC and are thereby able to review the results daily.
CYB_OS_41.	All vulnerabilities categorised as critical or high, will have been resolved within ten (10) Working Days of identification.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This process is covered by Meantime AMaT's ISO 27001 statement of applicability.
CYB_OS_42.	The resolution for all other vulnerabilities will be applied within a time scale agreed between the Authority and the Contractor, but no more than three (3) months.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This process is covered by Meantime AMaT's ISO 27001 statement of applicability.
Protective monitoring	
CYB_OS_43.	The Contractor must have a technical solution which proactively monitors the system and identify suspicious activity. This requirement is

Reference	Description
	in addition to a standard logging / monitoring system; it is specifically aimed at the identification of suspicious activity that could affect the security of the Authority's data. It should take a holistic approach, by examining logs & events from as many sources as possible. The Services will generate appropriate alerts and actions to be taken forward when potential indicators of compromise are detected.
Level of Compliance	**Supplier supporting statement**
Fully compliant	AMaT is a cloud-based system protected by Cloudflare which caters for this requirement.
CYB_OS_44.	The Contractor will commit to maintain the solution such that it remains up to date with known attacks vectors and indicators of compromise.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. This forms part of Meantime AMaT's ISO 27001 statement of applicability.
CYB_OS_45.	The Contractor will undertake regular reviews of the logs generated by the monitoring solution to analyse and produce trend data to pre-empt potential incidents or events from occurring.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. This process is covered by Meantime AMaT's ISO 27001 statement of applicability.
CYB_OS_46.	The Contractor will ensure that the monitoring solution has sufficient capacity to hold security information from network, infrastructure, applications and databases components within the Service for twelve (12) months so that investigation can be undertaken if required.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This process is covered by Meantime AMaT's ISO 27001 statement of applicability.
Incident management	
CYB_OS_47.	The Contractor will produce and maintain an incident response plan to deal with cyber security incidents. This plan is to be reviewed and tested on an annual basis to ensure that it remains up to date and appropriate for use.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 statement of applicability.
CYB_OS_48.	The incident response plan will include contact details for the designated Contractors cyber security personnel who are authorised, trained and equipped to respond to cyber-security incidents and will be available 24x7x365.
Level of Compliance	**Supplier supporting statement**

Reference	Description
Fully compliant	Confirmed. This forms part of Meantime AMaT's ISO 27001 policies and procedures.
CYB_OS_49.	The Contractor will notify the Authority, without undue delay, upon becoming aware of a security incident, which has either affected or has the potential to affect the confidentiality, integrity or availability of the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	In the event of a cyber incident, Meantime AMaT would: • Activate the system downtime message on mPire if it's an outage or cyber incident • Communicate to the Super User Group via standard channels • Follow our BCP which forms part of our ISO27001 statement of applicability.
CYB_OS_50.	Upon becoming aware of a Cyber Security incident, the Contractor will immediately take all necessary steps to: • Report – Notify the Authority of the incident, together with target timescales for response, containment & remediation. • Respond – Fully investigate the incident, identify whether or not a breach has occurred and if so the extent of the breach. • Contain – Identify the cause of the incident and take immediate action in order to minimise further impact. • Remediate – Identify, implement or improve controls to reduce the likelihood and / or impact from future events.
Level of Compliance	**Supplier supporting statement**
Fully compliant	In the event of a cyber incident, Meantime AMaT would: • Activate the system downtime message on mPire if it's an outage or cyber incident • Communicate to the Super User Group via standard channels • Follow our BCP which forms part of our ISO27001 statement of applicability.
CYB_OS_51.	Upon becoming aware of a security incident as outlined above, the Contractor will undertake any actions or changes reasonably required by the Authority to mitigate the effect.
Level of Compliance	**Supplier supporting statement**
Fully compliant	In the event of a cyber incident, Meantime AMaT would immediately begin an investigation and implement a solution, as per the BCP.
CYB_OS_52.	In the event that action is taken in response to a breach that is determined by the Authority, acting reasonably, not to be covered by the obligations of the Contractor under this Agreement, then the

Reference	Description
	Contractor shall be entitled to refer the matter to the Change Control Procedure.
Level of Compliance	**Supplier supporting statement**
Fully compliant	We are happy to agree to this but would appreciate more information on the change control procedure.
Configuration and change management	
CYB_OS_53.	The Contractor will maintain a complete inventory of assets used as part of the Service. The inventory will define the ownership and classification of each asset and will define appropriate protection responsibilities.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 statement of applicability.
CYB_OS_54.	When maintaining equipment within the scope of the Service(s), the Contractor will ensure continuous availability and integrity in accordance with original equipment manufacturers suppliers recommended service intervals and specifications.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 statement of applicability.
CYB_OS_55.	The Contractor will ensure that any software frameworks, used as part of the solution, are kept up to date so that they remain under the manufacturers support and that patches/updates can be received. The Contractor will identify and implement an upgrade path, no less than twelve (12) months before the end of general support, of the framework.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed.
CYB_OS_56.	The Contractor will ensure that Hardware, Authority Data and Software is not taken or removed from agreed locations without prior authorisation and will maintain records of all assets throughout their lifecycle.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Not applicable. AMaT is a cloud-based system.
CYB_OS_57.	The Contractor will implement a change control process and apply it to all changes within the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. This forms part of Meantime AMaT's ISO 27001 policies and procedures.
CYB_OS_58.	The change control process will include a Cyber Security view and will make an assertion on the level of risk presented.

Reference	Description
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. This forms part of Meantime AMaT's ISO 27001 policies and procedures.
CYB_OS_59.	The Contractor will notify the Authority when the risk review identifies a change in the level of risk the Contractor System has as a result of a change.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 policies and procedures.

Personnel security

Reference	Description
People and security culture	
CYB_PS_60.	The Contractor must ensure that there are control measures in place to manage and limit the roles which have access to Authority data and/or administrative access to the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 policies and procedures.
CYB_PS_61.	The Contractor must ensure that roles with access to Authority data and administrative access to the Contractor System are aware of their responsibilities to protect the data as set out in this schedule and have received specific training prior to being provided access.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. This forms part of Meantime AMaT's ISO 27001 policies and procedures.
CYB_PS_62.	The Contractor must maintain a list of all personnel who have access to Authority data and/or administrative access to the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 statement of applicability.
Technical controls for service administration	
CYB_PS_63.	The Contractor must conduct pre-employment screening against all staff who will have access to the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 statement of applicability.

Reference	Description
CYB_PS_64.	The Contractor must ensure that all administrative actions performed by staff are recorded within an audit system.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. This forms part of Meantime AMaT's ISO 27001 policies and procedures.
CYB_PS_65.	The Contractor must conduct regular reviews of the audit logs to ensure that all actions are performed as part of an approved change.
Level of Compliance	**Supplier supporting statement**
Fully compliant	N/A. Our change control policy would only allow work to be done as part of an approved change.

Secure development

Reference	Description
CYB_SD_66.	The Contractor will maintain documented security requirements covering secure development, deployment and configuration and will ensure minimum security baselines are applied to all developments.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 statement of applicability.
CYB_SD_67.	The baseline security requirements must be documented and periodically reviewed to ensure they remain fit for purpose.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Meantime AMaT's ISM forum meets monthly to review all aspects of its security requirements and processes.
CYB_SD_68.	The baseline security requirements must follow an industry recognised standard, e.g., CCM.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed.
CYB_SD_69.	The Contractor will ensure that confidential Authority data is not used for test, development or training purposes.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Meantime AMaT is fully compliant with GDPR when it comes to the use of test data.
CYB_SD_70.	The Contractor will ensure that there is enforced separation between the environments used for the live system and other purposes, such as development, training, and testing.
Level of Compliance	**Supplier supporting statement**

Reference	Description
Fully compliant	All instances of AMaT are separate.
CYB_SD_71.	The Contractor will use, where possible, automated process for the configuration and deployment of releases into the live instance of the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 policies and procedures.
CYB_SD_72.	The Contractor will pay particular attention to Security risks associated with the use of third-party software and libraries and will ensure that supported versions are used at all times.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 statement of applicability. Third-party software and libraries is at a bare minimum. Nearly all software is written by Meantime AMaT.

Supply chain security

Reference	Description
CYB_SCS_73.	The Contractor must ensure that Authority data is not shared with any third parties without prior approval from the Authority.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Meantime AMaT does not share data with any third parties.
CYB_SCS_74.	If approval has been granted by the Authority for the data to be shared with a (any) third party, then the Contractor will ensure that the conditions as defined this in schedule are passed onto the third party and must be adhered to.
Level of Compliance	**Supplier supporting statement**
Fully compliant	If, for any reason, the organisation wished to share data with another party it would be up to them to put data sharing agreements in place and work with Meantime to make the sharing possible through specific APIs.
CYB_SCS_75.	The Contractor will ensure that their risk management process pays particular attention to risks from within their supply chain.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 statement of applicability.

Secure user management

Reference	Description
CYB_SUM_76.	The strategic objective of the Authority is for all system authentication and authorisation to be performed by the NHS Wales authentication system. The supplier must provide an alternative solution is this is not achievable.
Level of Compliance	**Supplier supporting statement**
Fully compliant	AMaT supports single sign on with username and password as a fallback.
CYB_SUM_77.	The Contractor will ensure that access control system restricts functions of the Services to specific roles associated with users.
Level of Compliance	**Supplier supporting statement**
Fully compliant	AMaT has specific user roles and operates on the principle of least privilege. NB: Access to specific types of data (PID) and one module (MaMR) is restricted to one specific user role.
CYB_SUM_78.	The Contractor will ensure that access requests (successful & unsuccessful) to the Contractor System will be stored and made available for audit.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. This information is available via a report which is available to super users.
CYB_SUM_79.	The Contractor will ensure that access is provided on the basis of Least Privilege and will only grant access to users who have a legitimate need to have access.
Level of Compliance	**Supplier supporting statement**
Partially compliant	Access is provided on the basis of least privilege. However, access is granted by the organisation either by approval of registration or active directory.
CYB_SUM_80.	The Contractor will ensure that access is provided for the minimum amount of time required to perform the task.
Level of Compliance	**Supplier supporting statement**
Partially compliant	AMaT is not a task-based system. However, the organisation is able to rescind access without recourse to Meantime AMaT.
CYB_SUM_81.	The contractor system must be protected with account lockout/session timeouts appropriate to the environment in which the system will be deployed.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed. This has been agreed upon by the super user group.

Reference	Description
CYB_SUM_82.	All accesses to the Contractor System must be authenticated. If access provides any level of administrative access, then MFA must be used.
Level of Compliance	**Supplier supporting statement**
Fully compliant	For organisations using single sign-on, access is managed via Active Directory although the user's role is managed within AMaT. Where a Trust is not using single sign-on, automatic registration is possible for Trusts with their own email domain. If a generic email domain (such as nhs.net) or private email address is used, then registration must be authorised by an administrator. MFA is available to organisations that have implemented single sign on.
CYB_SUM_83.	All accesses to the Contractor System must be authenticated by MFA when access is permitted from the internet.
Level of Compliance	**Supplier supporting statement**
Fully compliant	MFA is available to organisations that have implemented single sign on.
CYB_IAA_84.	The contractor should utilise cloud managed service accounts where possible/appropriate, any user managed service accounts should conform to the following: • Strong credentials (20 characters, regularly changed) • Adhere to the principal of least privilege • Have no access to administrative/ privileged groups • Be monitored (sign-in activity/ misuse) • Regularly review & clean up Service Account
Level of Compliance	**Supplier supporting statement**
Partially compliant	All confirmed apart from password length which is currently set to 15 characters on the request of our super user group.

Identity and authentication

Reference	Description
CYB_IAA_85.	The Contractor will ensure that all interfaces to the Contractor System are protected with Authentication, authorisation, and Encryption, this applies to user access (where required) as well as service interfaces.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed.

Reference	Description
CYB_IAA_86.	The Contractor will ensure that it has a strong password policy protecting access to the Contractor System.
Level of Compliance	**Supplier supporting statement**
Fully compliant	Confirmed.

External interface protection

Reference	Description
CYB_EIP_87.	The Contractor will maintain a list of all external interfaces to the Contractor System along with details of the controls that are used to protect them.
Level of Compliance	**Supplier supporting statement**
Fully compliant	N/A
CYB_EIP_88.	The Contractor will implement a technical solution which provides a consistent level of protection for all external interfaces.
Level of Compliance	**Supplier supporting statement**
Fully compliant	N/A
CYB_EIP_89.	The Contractor will minimise the number of Components to be trusted, by reducing the attack surface.
Level of Compliance	**Supplier supporting statement**
Fully compliant	N/A

Secure service administration

Reference	Description
CYB_SSA_90.	The Contractor will ensure that all administrative access to the Contractor System is performed only from trusted, corporately managed devices.
Level of Compliance	**Supplier supporting statement**
Fully compliant	This forms part of Meantime AMaT's ISO 27001 policies and procedures.

Audit information and alerting for customers

Reference	Description
Audit information	
CYB_AIA_91.	The Contractor will ensure that the audit system described in section "Protective Monitoring" CYB_OS_43 will hold sufficient information to enable a thorough and robust investigation to take place and identify any malicious activity.
Level of Compliance	**Supplier supporting statement**
Fully compliant	AMaT is protected by Cloudflare and Microsoft Defender and all activity is logged.
Security alerts	
CYB_AIA_92.	The Contractor will ensure that the monitoring system described above will be sufficient to detect attacks against the Contractor System and will raise alerts for review.
Level of Compliance	**Supplier supporting statement**
Fully compliant	AMaT is protected by Cloudflare and Microsoft Defender.