دائـــرة الـصـحـــة
DEPARTMENT OF HEALTH

FREQUENTLY ASKED QUESTIONS (FAQs)
Abu Dhabi Healthcare Information and Cyber Security

Frequently Asked Questions

1. What is ADHICS Audit Program?

Reference to the enforcement of Abu Dhabi Healthcare Information and Cyber Security Standard, through “Circular No. US/14/19” (Abu Dhabi Healthcare Information & Cyber Security Standard) dated 18th March 2019, and as per ‘Circular No. USO/71/20 dated 19th July 2020, DoH shall initiate an audit program to validate healthcare entity’s compliance towards ADHICS Standard, as applicable and as relevant.

The audit program shall be executed by TASNEEF through their subsidiary TASNEEF RINA Business Assurance. The following cyclic audit approach will be adopted:

- Year 1 – Certification audit
- Year 2 – Surveillance audit 1
- Year 3 – Surveillance audit 2

Second cycle:
Recertification
Surveillance
Surveillance

Based on successful audit completion during year 1, healthcare entity shall be provided a certificate on conformance valid for three years, and the audit program will be repeated on a three-year cycle

2. Which are the main deadlines I need to consider?

As you receive the notification for Kick off from a dedicated system, you must upload certain information like personnel nominated, general and technical questionnaire, in a dedicated system as Audit tool, within 5 working days.

You will receive an audit plan after that, and you will be requested to upload documentation in the Audit tool within 5 working days for TASNEEF desktop audit.
Interviews will be conducted in specific dates after desktop audit.

3. Is it mandatory and to whom?

Yes, this certification is mandatory for all applicable entities indicated in ADHICS standard.

Eligible or nominated groups, batch or type of healthcare facilities, parties, entities, will be identified annually by a circular or official information from Department of Health (DoH), even though the ADHICS standard shall be implemented by all healthcare facilities as per the standard’s specifications.

4. Which facilities are in scope of audit?

The ADHICS certification pertains exclusively to:

- A single healthcare facility identified by its DoH license number or
- Group of facilities belonging to a main ‘pivot’ entity (as identified by DoH)
- Individual entity/ professional/ third party administrator/ insurance company

ADHICS covers all DOH regulated health care entities and services within the Emirate of Abu Dhabi, and is extended also to any third parties involved in healthcare

- Applicable to all healthcare/medical facility(s), healthcare professional(s) and support staff who have access to patients’ health/diagnostic/personal information, diagnostic lab(s), pharmacy(s) and insurance provider(s).
- Hospitals
- Centers (Day Care Surgery Center, Primary Health Care, Diagnostic Center, Rehabilitation Center, Dialysis Center, Fertilization Center, Mobile Healthcare Unit, Provision of Health Service /Home care)
- Pharmacy Establishment as Drug Store (Medical store)
- Professionals
- Insurance companies
- Third parties’ Administrators/ other applicable parties

5. Which are the criteria of the audit?

Audit will cover Section A and Section B of ADHICS standard, including controls in Section B.

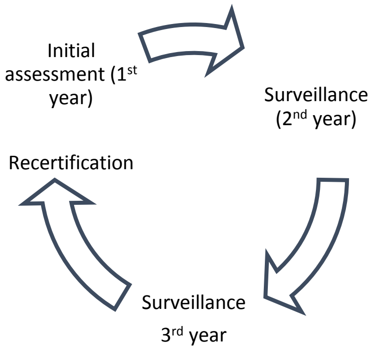
6. Is the audit scope same to a small clinic compared to any hospital?

In relation of facility type, three categories of controls are identified as:

- Basic (applicable to all facilities)
- Transitional
- Advanced

7. Is it a one-time audit or to be repeated?

The minimum audit time is assigned by categories/ batches/ groups. Certification Cycle will be for 3 years followed by Recertification Audit. Domains could be audited not in the same time but in three years.



Audit phases are distributed through the stage 1 and stage 2.

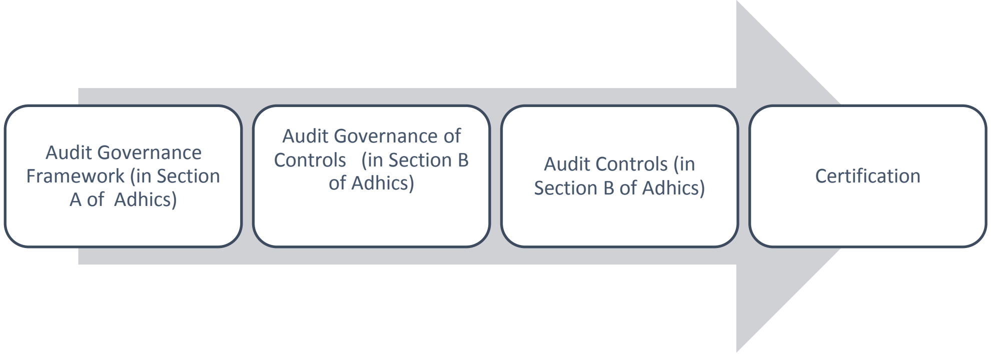
a) Stage 1

- Phase 1 - Audit on Section A
- Phase 2 – Audit on Section B in regard of Policies as Governance of Controls

b) Stage 2

- Phase 3 – Audit on Controls

Phases can be audited consequently or in different schedules/periods.


Audit Governance Framework (in Section A of Adhics)
Audit Governance of Controls (in Section B of Adhics)
Audit Controls (in Section B of Adhics)
Certification

8. When will the audits start?

Audits will start from September 2020 for specific entities identified by DoH.

9. Does the facility have to pay for the audit?

Not for 2020, eventually from 2021 as per DoH decisions.

10. Which department in our facility is related to this audit?

- Information Security / IT Department as main department and additional departments may be involved at certain times of implementation.
- Presence of Top management for the closing meeting is important to show the commitment to continual quality improvement of organization and to understand the areas of improvement and actions.

11. Is there any reference standard for this audit?

Yes, Abu Dhabi Health Information and Cyber Security Standard

12. Is the audit conducted by DoH or TASNEEF?

The audit will be conducted by TRBA, subsidiary of TASNEEF, and DoH will be closely involved and monitoring the process and outcomes.
ADHICS Certification will apply a third-party concept audit.

13. How is the auditee informed about the audit schedule?

Auditee will be informed by a kick off communication and by an audit plan, with the schedule of the dates related to audit activities, that can be assessment for certification, surveillance, or recertification audit.

14. What are the pre-requisites for this audit?

Following information should be submitted to DoH

- Facility self-assessment (quarterly submissions or at least the latest submission)
- Facility Malaffi security assessment submissions
- Updated General information and Technical Questionnaire.

Below information should be provided by an authorized representative of the applicant organization that shall be the point of contact for the entire certification process.

A Technical questionnaire will be sent including but not limiting to the below information (ref. Information Security Management System [Isms] Questionnaire)			
Status of Malaffi integration/ data exchange	To be specified the activities company is actively running as whole, and those provided	Corporate or Third Party to specify the number and type of healthcare	Activities or outsourced processes and if Coding/claims submissions are also outsourced

	to Healthcare facilities as Corporate or as Centralized Administration or as Third Party	facilities to which they provide services		
Name of EMR & Name of EMR vendor and information if cloud based or on-premises	Information on 3rd party services utilized and type of such as: □Third Party Administrators □ Service vendors such as IT etc. To be included a list of 3rd party vendors and scope of work if utilized.			
Number of servers and platforms	Number and type of management systems implemented and certified	If there is a Valid certificate in information security management system (e.g. ISO 27001)	Information on Outsourcing of platforms, tools.	Total number of personnel Number of personnel involved in IT and in Information & Cyber Security

- Facility must share the facility location and contact details along with location map and landmark.
- All correspondence will be sent by registered emails only, and changes must be notified to TASNEEF.
- Requests of evidence of supporting documentation, and identified deviations should be provided
- Any required approvals or permissions to provide evidences should be obtained prior to the audit process.
- It is highly recommended to provide evidence in electronic format to save paper and time.
- It is the responsibility of the auditee to provide all the evidence by documentations requested during the audit
- Failure to provide the requested evidence within the audit day and time shall be considered as non-compliance with certification requirements and any documentations provided for any reason after the timelines cannot be accepted. Audit and or certification process for such facilities may be stopped, as the audit process will be use-less and ineffective

15. Is there an audit plan and when do we receive it?

i. An "Audit Plan" is drawn up for each audit. A different audit plan is prepared for Stage 1 or Stage 2 audit

ii. An audit plan will be communicated to the auditee 2 weeks before the date for interviews or even prior.

iii. The auditee is required to share the list of personnel in details and in the scope of audit, for interviews at least 3 weeks prior to the date of interviews.

16. What does the audit plan constitute?

The audit plan indicates:

a) Scope and size, sections of ADHICS, domains and controls to be audited

b) The structure, policy, processes, records, and relative documents to the applicable ADHICS management system to verify:

The audit plan will also define:

- if it is performed onsite or offsite
- No. of auditors
- dates and duration
- agenda/schedule
- if it is linked to other entities/sites

17. Is the audit conducted onsite or remotely?

The auditing team may decide to perform any audit as partially on site and partially as desktop/remotely according to the best efficient mode or best safety and security options.

18. Can we know more about the audit program?

i. Every year an audit program will be prepared, communicated, and updated at the end of the audit

ii. There are 2 stages in audit: Stage 1 Audit and Stage 2 Audit

Stage 1 will include

- Audit on Governance Framework: Section A of ADHICS Methodology Part 1 (Standard)
- Governance of Controls (Policies): Section B of ADHICS Methodology Part 1 (Standard)

Through:

- Desktop Audit: Documental review of policies (Desktop audit result will be communicated by a report with observations to be corrected eventually
- Remote Audit (by remote connection between auditors and auditee)

Stage 2 will include

- Audit on Controls implementation- Section B of ADHICS Methodology Part 1 (Standard)

Through:

- Desktop Audit: Documental review of controls
- Remote Audit (by remote connection between auditors and auditee)
- And/or by onsite Audit

i. Before the Audit, auditee will be requested to send soft copies of the pre identified policies or other documents that constitute requirements of ADHICS.
ii. Review will be performed from TASNEEF team as part of the Stage 1 as desktop audit, to make a documental review.
iii. After the completion of Stage 1, Auditees will be requested to send soft copies of the documents constituting part of stage 2 documental review, as desktop audit.
iv. On the planned dates, auditees shall be available for interviews, videocalls, and other remote audit aspects, or for clarifications about aspects of the management system, remotely connected for Stage 1, or by onsite visit during Stage 2, if not performed also fully remotely.

19. How many days the audit will happen?

- For hospitals, third parties, insurance companies (and all those identified by DoH as in the same complexity and risk, or in the same batch), the audit time will be minimum 5.5-man days for first certification/ initial assessment and 2.5-man days for surveillances. For other entities time is more limited.

20. Can the audit time be extended?

Yes, audit time may be extended due to below factors

i. Factors related to operational size
   - Factors/weights related to IT environment: Identified by the categories of controls in the standard and they correspond to:
   - Transitional
   - Advanced

ii. Multi-Site Facilities or Groups

This is the scenario when providers operate more than one facility, entities/ parties, or when can be identified a centralized system controlling multiple sites, and it’s necessary to verify some of these sites to confirm the cohesion of the systems.

21. How is the audit conducted for a group of facilities with certain functions as centralized?

- This is the scenario when providers operate more than one facility, entities/ parties, or when can be identified a centralized system controlling multiple sites, and it’s necessary to verify some of these sites to confirm the cohesion of the systems
- For Groups of auditees, Certificate will report the extensions or exclusions of the audit performed (e.g. sites, functions, etc.)
- In case of centralized systems for group of facilities/entities/parties, the auditor will verify centrally on other controlled entities following same methods and procedures in adherence of the centralized policies and their processes accordingly.

22. What are the domains and control categories applicable for audit from the ADHICS standard?

The auditee must make all necessary information available to TASNEEF.

Certification Process will generate a scoring and an evaluation of the level of maturity of the system, so a certification grade will be generated.

Audit is based on third party model and sampling style, so score will not be intended as reflecting the full compliance on whole aspects and requirements.

Controls’ categories
Basic Control Implementation
Transition Control Implementation
Advance Control Implementation

Governance Framework domains - Section A of ADHICS (numeration reflecting the chapters)
3) Governance Structure
4) Risk Management
5) Asset Classification
6) Control Adoption, Compliance and Audit
7) Healthcare Entity Responsibility

Governance and Control domains – Sections B of ADHICS	
1) Human Resources Security	7) Health Information and Security
2) Asset Management	8) Third Party Security
3) Physical and Environmental Security	9) Information Systems Acquisition, Development, and Maintenance
4) Access Control	10) Information Security Incident Management
5) Operations Management	11) Information Systems Continuity Management
6) Communications	

23. How the findings are categorized?

Outcome and findings categorisation	Definition
Not Applicable	The control requirements are not relevant to the entity and may not impact entity's risk environment. Entity shall provide adequate justification, while selecting this control status. Can be referred also to the case of non-applicable to the audit in case certain domains will be not audited (justification to be provided by the auditor in this case).
Compliant	The control/sub-control is fully implemented, has been established and has a process, and is regularly updated. It has an objective evidence of effectiveness implementation of the standard requirement.
Partially Compliant	The control/sub-control is implemented but not across all of the entity's information systems, and a process has not been fully established, or is outdated. It represents an issue, resolution of which would improve overall effectiveness / efficiencies of the process. It is usually the outcome of non-systematic approaches and could lead to a strategic impact.
Not Compliant	The control/sub-control is not planned nor implemented. A fundamental or important issue that requires an action as soon as possible without which a process may result in unproductive or ineffective outcome and high impact. It is usually the outcome of requirements completely not met and total absence of systematic approach, with a strategic impact.

24. What should be done for non-compliant findings?

- In all cases and grades, healthcare facilities may have the presence of noncompliance.
- For all grades it is required to present a corrective action plan.
- In case of Grade C, the evidence of implementation of corrective actions must be presented within 90 days but certification will be granted.
- In case of score less than 86, healthcare facilities will be subject to a further evaluation from DoH.

25. What is the passing score for the audit and is there any grading system?

The current passing score is 86% as an overall score and as average of the scoring of 11 controls domains.

Score	Grade
96-100	"A" (system certified and optimized)
91-95	"B" system certified and optimized
86-90	"C" system managed and optimized
<86	Not certified

26. How to interpret results of entities with <86%?

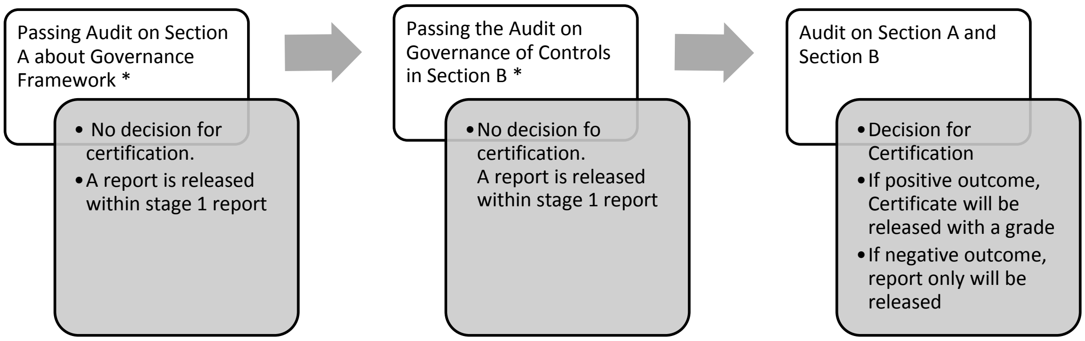
Non certifiable organizations (entities, facilities, parties) will be receiving a report and eventually a statement with Maturity level, as reported below:

Maturity Level < 86%	
Compliance Percentage	**Maturity**
0 - 30 %	**Initial**
31 - 55 %	**Repeatable**
56 - 75 %	**Defined**
76 - 86 %	**Managed**

27. Will any certificate be issued after audit?

- The issuing of certifications is a responsibility of TASNEEF and DOH based on Certification Committee decision.
- Certificate is not a public information
- The Certification Expiry Date is based on three years from the date of first decision, however grade shall be updated in case of change and history of grades reported in a specific annex.
- For Groups of auditees, Certificate will report the extensions or exclusions of the audit performed (e.g. sites, functions, etc.)

Decision of certification has the following levels of outputs:



Passing Audit on Section A about Governance Framework *

- No decision for certification.
- A report is released within stage 1 report

Passing the Audit on Governance of Controls in Section B *

- No decision fo certification.
  A report is released within stage 1 report

Audit on Section A and Section B

- Decision for Certification
- If positive outcome, Certificate will be released with a grade
- If negative outcome, report only will be released

28. Can the certificate once issued, be revoked?

- Auditee must ensure its System continues to comply with the Standard. Validity is confirmed by annual audits of surveillance. Refusing or not performing surveillance audits is reason of suspension and eventually revoke and withdrawn of the certificate.
- TASNEEF may conduct a follow-up audit to confirm that the major deviations identified during the audits have been corrected by facility as per the action plan. If the facility refuses without a justified reason, Certification Committee may decide to suspend/withdraw certification.
- if the Facility/ Entity or Party refuses to allow the scheduled audits;
- if observations are found in the management system which have not been corrected within the time limits established;
- if the facility does not observe the deadlines established for the communication of corrective actions, following observations/observations indicated on the audit report;
- for evidence that the facility does not guarantee the respect of the laws and regulations applicable to the supplied services or activity;
- if any justified and serious claims received by TASNEEF or DoH are confirmed;
- for every other major reason, at Certification committee decision, such as the proven incapacity of the system to pursue its objectives of complying with legislative, contractual requirements and other aspects mentioned in these rules

29. What is the impact of failed audit?

- Failing certification audit will be in general having consequence to repeat initial certification audit in the next year.
- A re-audit may be conducted within 30 calendar days to verify the implementation of corrective actions and their effectiveness, considering that Re-audit will be done only for the problem area. Re-audit will be performed in 1 day and when applicable, cost will be charged separately.

30. Are there any Ad-Hoc audits?

Ad Hoc audits can be executed when market surveys, DoH concerns, or specific incidents need to be verified.

31. Can the certification process be suspended?

- In cases when the auditee cannot provide the evidence before the completion of the audit time.
- In cases when TASNEEF will reject the facility proposed corrective actions not resulting in effective solution for identified noncompliance.
- In case of not sending the corrective actions plan in the 10 working days from sending the findings of noncompliance.

32. What are the conditions at which audit process will stop?

- When required evidence of compliance is not provided on time.
- When the planned nominated personnel are not available and or the not competent to provide support.
- Absence of authorized person from the top management to facilitate the audit process.
- Any case that might be classified by the lead auditor as a reason such as:
  - 1.1...1. Unavailable agreed resources
  - 1.1...2. Unavailability of required employees
  - 1.1...3. Any interaction from unnominated auditee which will not pour in the sake of audit and may adversely effect on the auditor ability to conclude proper and professional conclusions.
- If due to emergency situations TASNEEF auditors could not join the audit as per the planned arrangements client will be communicated to set another audit plan

33. Can you provide an example of evaluation, scoring and grading?

Example of evaluation, scoring and grade

The Final ADHICS Data Certification Score will be a comprehensive score obtained as per the average of assigned scoring weights for each domain, with reference to the Self-Assessment Check list dated 19th of Feb.2019.

Any requirement stated as not applicable from auditee, but found applicable, will be scored as fully compliant, partially, or not compliant according to the case.

Check outcome and findings categorisation	Definition
Not Applicable	The control requirements are not relevant to the entity and may not impact entity's risk environment. Entity shall provide adequate justification, while selecting this control status. Can be referred also to the case of non-applicable to the audit in case certain domains will be not audited (justification to be provided by the auditor in this case).
Compliant	The control/sub-control is fully implemented, has been established and has a process, and is regularly updated. It has an objective evidence of effectiveness implementation of the standard requirement.
Partially Compliant	The control/sub-control is implemented but not across all of the entity's information systems, and a process has not been fully established, or is outdated. It represents an issue, resolution of which would improve overall effectiveness / efficiencies of the process. It is usually the outcome of non-systematic approaches and could lead to a strategic impact.
Not Compliant	The control/sub-control is not planned nor implemented. A fundamental or important issue that requires an action as soon as possible without which a process may result in unproductive or ineffective outcome and high impact. It is usually the outcome of requirements completely not met and total absence of systematic approach, with a strategic impact. It is equal to a major finding and when related to a basic control, it’s also cascading in the category of high risk in controls for those entities eligible for transitional and advanced controls.

Scoring will be considering all requirements in the Section B both for the Policies/ Governance and Technical controls and sub controls. Scoring is considering the stage 2 only. Example of simulating as following:

Case of controls checked for a group of entities/facilities. In this example

Domains	Controls checked in the primary/centralized/corporate entity	Controls checked also in sampled entity belonging to the group	Maturity
Human Resources Security	10	2	86%
Asset Management	9	0	86%
Physical and Environmental Security	7	3	83%
Access Control	0	1	Not checked any point (not valid for the average)
Operations Management	23	2	71%
Communications	11	6	83%
Health Information and Security	15	4	33%
Third Party Security	6	3	86%
Information Systems Acquisition, Development, and Maintenance	21	4	95%
Information Security Incident Management	4	2	100%
Information Systems Continuity Management	32	8	86%
Final score			80.9%

Control Summary for the maturity level and certification grade	
Overall Implementation (average of the scores from domains)	80.9%

1. The simulation has shown a score of 80.9%. According to the below Table the Group of Facilities/ Entities/ Parties will not be considered as certified but will have a statement as 'System Managed' only.
2. Being a group or a corporate, where management of strategies and preparation and implementation of policies is centralized, the audit on Section A and Section B (regarding Policies and Governance of Controls) must be conducted in the centralized function as primary entity. When the group of two for example, has different corporate functions and information security management, still the final score and grade will reflect the average of the two.

Table for scoring grades

Maturity Level		**Certification grades**
Compliance Percentage	**Maturity**	**Grade**
0 - 30 %	Initial	
31 - 55 %	Repeatable	
56 - 75 %	Defined	
76 - 90 %	Managed	Grade C =>86-89%
91 - 100 %	Optimized	Grade B=>90-95% Grade A=>96-100%