دائـــــرة الـــصـــحـــة
DEPARTMENT OF HEALTH

CERTIFICATION RULES 2020 (Abu Dhabi Healthcare Information and Cyber Security Standard)

July 2020

دائـــرة الـصـحـة
DEPARTMENT OF HEALTH

Document Title:	Certification Rules – Abu Dhabi Healthcare Information and Cyber Security Standard
Document type	Framework
Document Ref. Number:	DOH/SD/CR/0.9
Effective Date:	The effective date of this framework will be the date of its publication.
Previous versions	None
Document Owner:	Support Services Division
Applies to:	• 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

This Framework should be read in conjunction with related UAE laws, DOH Standards, Policies and Manuals including but not limited to:

- Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS).

TABLE OF CONTENTS

1 GENERAL

These Rules are about the Abu Dhabi Healthcare Information and Cyber Security Standard (herein after referred to as "ADHICS") Certification. These rules describe how the eligible or nominated entities can or must apply for obtain and maintain ADHICS certification. These rules are not public, and they shall be considered as restricted information for the facilities, entities, and parties eligible, nominated or identified from DoH for ADHICS Certification.

1.1 Certification Methodology

Certification Methodology is composed by:
Methodology Part 1: Part 1 is the Abu Dhabi Healthcare Information and Cyber Security (ADHICS) Standard (DOH/SD/ADHICS/0.9) dated 3rd February 2019. Methodology part 1 is the reference for the management system (including also controls) requirements of the ADHICS certification, including also those references reported in Appendix 5 of the Standard itself.
Methodology Part 2: it is formed by Certification Rules and its revisions.

1.2 Applicability

The ADHICS Standard sets out the minimum requirements of controls, essential to secure healthcare information. Certification is open to Healthcare facilities in Abu Dhabi belonging to the following list. ADHICS Methodology covers all DOH regulated health care entities and services within the Emirate of Abu Dhabi, and shall be 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). However, ADHICS certification is extended also to any third parties involved in healthcare.
List:

- 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

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

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

1.2.1 Organizations eligible or nominated for certification

Certification will involve facilities, entities, and parties by a progressive plan or batches. In these Rules, such organizations are also referred to ‘auditee’.

1.2.2 Initial Phase for Certification

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.

1.2.3 Certification may be refused to facilities or entities whose activities have been subject to restriction, suspension, or proscription by a public authority.

When TASNEEF declines an application, the reasons shall be communicated to DoH and to the facility CFO/CEO/COO or delegated authority including the representative for audit.

1.2.4 This document also describes the certification process. ADHICS Certification will apply a third-party concept audit.

1.2 Certified Entity

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

1.3 Limitation of responsibility and liability

According to the international practice of third-party certification, the audits will be based on sampling method and certification will not exempt the auditee from its liabilities and responsibilities from operating, implementing, and improving the ADHICS Standard. TASNEEF and DoH will not be liable in case of accidents and incidents pertaining to the auditee and other relevant parties related or involved, in regard of Information and Cyber Security. ADHICS Certification does not constitute an exemption or transfer of liabilities and duties.

2 PLANNING FOR CERTIFICATION

2.1 ADHICS Certification

The objective of certification is evaluating the level of implementation of ADHICS among the healthcare community.
To obtain ADHICS Certification the auditee must:

- Have established a Management System and kept it active in total compliance with the requirements of the ADHICS Standard
- The management system is considered as being fully operative and implemented when processes, controls and documented information are established and maintained for the requirements of the standard.

2.1.1 Audit domains and category of controls:

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 judgmental style, so score will not be intended as reflecting the full compliance on whole aspects and requirements.

Hereinafter the audit domains and control categories of the Standard, applicable to certification.

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

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	

Controls' categories
Basic Control Implementation
Transition Control Implementation
Advance Control Implementation

Auditee will be informed by a planner or direct notifications on the dates and periods related to the first certification audits.

Auditee will be informed at the end of initial certification on surveillances, or recertification audit.

In planning for certification, following information should be available or collected, if not yet available from DoH systems:

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

Before the audit, the auditee will be requested to update or upload certain information that are reported below as General Information and as Technical Questionnaire. Such information could be sent to DoH dedicated system. To execute the audits, Self-Assessment will require and include also uploads of the documents as evidence of the self-assessment, as selected from the CB during the Audit plan, to be utilized as audit documentation as well. Such uploads may be executed directly in the DoH dedicated platform.

In case of any payment to be released to DoH or TASNEEF, it will be settled before the audit.

Below the tables for the General Information to be communicated, and the Technical Questionnaire.

Entity Name/Group reference:
DoH License/s No.
Entity Location (for Groups is the corporate of the Group):
Type of Facility (if it is a Group, should be listed all types of facilities under the group): * Hospital with XX number of beds * Center (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 * Third party administrator/ entity/party
Name of Chief Executive Officer (CEO) or equivalent:
Email Address of CEO:
Phone Number of CEO:

Name of Chief Information Security Officer (CISO) / Chief Cyber Security Officer (CCSO):
Email Address of CISO / CCSO:
Mobile Number of CISO / CCSO:

Name and Contact Details of Information Security Governance Committee (ISGC) Members				
Name of ISGC Member	Role (Chairperson / Co-Chairperson / Committee Member)	Title	Email Address	Phone / Mobile Number

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 to Healthcare facilities as Corporate or as Centralized Administration or as Third Party	Corporate or Third Party to specify the number and type of healthcare facilities to which they provide services	Activities or outsourced processes and if Coding/claims submissions are also outsourced	
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

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

All correspondence will be sent by registered emails only, and changes must be notified to TASNEEF.

2.2 Pre-Audit Activities

When applicable:

i. ADHICS certification will be charged to facilities/ entities/ parties as per the applicable category and man days

ii. TASNEEF will communicate the contractual documents to be returned 45 days before the audit. Contract will automatically be assigning the activities for ADHICS certification that are mandatory for those facilities identified in the related circular or information and planner. This is not applicable when activities are not chargeable to facilities/ entities/ parties/ administrators.

When applicable on receipt of the contract for certification and having ensured they are complete, TASNEEF will send the auditee written acceptance of its application, proceeding to generate the invoice along with other additional steps for the audit process.

When fees charge are not applicable directly, but cost is supported by authorities, auditee must ensure the best of commitment also from pre audit communications onward.

2.3 Audit Planning

- The entity (following ref. as the auditee) will be required to share the list of personnel in details and in the scope of audit (personnel as owners of the controls) , for interviews in five working days from the notification (ref. project kick off communication).
- Any request for re-schedule should be sent at least 1 month before with documented reason for request. In the absence of very significant reason, the schedule will not change, and the audit will proceed as per the schedule. In case of unjustified deviation from the planner, cost of the audit will be borne by the entity. Reschedule request are not allowed for 2020 due to the constraints in timing.
- An audit plan will be communicated to the auditee within 2 weeks before the audit date (expected for onsite or online interviews) or even prior.
- 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.
- In addition, or integration of the latest Self-Assessment Submission, before the Audit, auditee will be requested to upload soft copies of the pre identified policies or evidence that constitute requirements of ADHICS. Review will be performed from TASNEEF team as part of the Stage 1 as desktop audit, to make a documental review.

- In addition, or integration to the uploads as evidence of the latest Self-Assessment Submission, After the completion of Stage 1, Auditees will be requested to uploads soft copies of the documents constituting part of stage 2 documental review, as desktop audit. In the dates highlighted in the planner Auditee and personnel governing the controls shall be available for interviews, video calls, 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.
- If the certification and audits are related to a Group, what will be identified as Primary or Pivot or centralizes entity will receive the main of the audit, with possibility to involve in the stage 2, a sampling of other facilities in the Group.

2.4 Audit time

The minimum audit time is assigned by categories/ batches/ groups. Certification Cycle will be for 3 years followed by Recertification Audit.

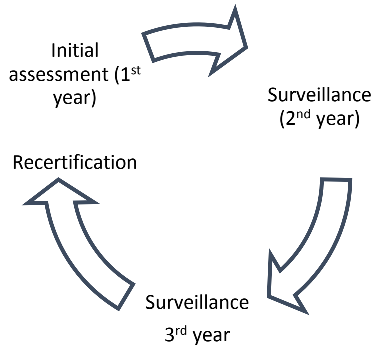


Figure – Three years audit program

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 5.5-man days for first certification/ initial assessment and 2.5-man days for surveillances.
For other entities Audit Time will be 1 man-day for first certification/initial assessment and following surveillances and recertification.
Domains could be audited not in the same time but in three years.

2.4.1 Reasons to extend audit time

2.4.1.1 Factors related to operational size

Such factors are considered as per volume of healthcare services provided, that are detectable by volume of claims visible in the JAWDA Sampling tool system, in the last 12 months from 3 weeks before the audit planned date.

2.4.1.2 Factors/weights related to IT environment:

Such factors are identified by the categories of controls in the standard and they correspond to:

- Transitional
- Advanced

2.4.1.3 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 is necessary to verify some of these sites to confirm the cohesion of the systems.

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.

3 CONDUCTING AUDITS

3.1 General

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

The audit has the following objectives and it is done by a sampling approach:

a) Audit criteria are defined by the standard
b) Determination of the compliance of the management systems, or part of it, with audit criteria
c) Evaluation of the ability of the management system to ensure the organization meets applicable requirements for information security and cybersecurity
d) As applicable, identification of areas for potential improvement of the management system.
e) Audit questions and requests to uploads documentation as evidence of implementation of policies and controls

The sampling method include all the controls audit across or along a cycle of 3-5 years, depending from complexity, applicability of controls, size of the scope and extension of groups, eventually.

3.2 Audit program

Every year a 3 years' plan audit will be prepared, communicated, and updated at the end of the annual audit, with controls in the scope for next year.

3.3 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, so to anticipate the reviews and to have a more efficient stage 1, also to reduce the compression of the audit done in remote connection).
- 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

3.4 Audit plan and audit focus

The Audit Plan indicates the tasks assigned for audit. Specifically, for each facility/ entity covering the applicable domains to check, audit plan indicates the scope and size, sections of Adhics, domains and controls to be audited, along with certain questions to be replied and demonstrated by documents during the desktop audit.

The audit plan will also define:

- if it is performed onsite or offsite
- auditors
- dates and duration
- agenda/schedule
- if it is linked to other entities/sites

Audit focus is on:

a) The structure, policy, processes, records, and relative documents to the applicable ADHICS management system to verify:
   a. whether these satisfy the requirements applicable
   b. whether the processes and documented information are drawn up, implemented, and kept efficient, to nurture trust in the management system;
   c. every inconsistency between the organization or policy, objectives, goals, and the result obtained

Communication along with the nominees mentioned on the audit plan are seen to be required for opening and closing meetings to ensure a clear understanding of the audit objective, process, identified findings and required corrective actions.

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.

3.5 Audit Process:

The audit process will be conducted as per the audit plan starting with collecting and/or review of soft copies uploaded in the DoH platform, by desktop audits. During assigned dates, audit will continue by an initial meeting, request for additional evidence, interviews with the staff, visiting sites when applicable and closing meeting.

3.5.1 Audit phases 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.

The process approach is to evaluate the Section A of the ADCHIS Standard to verify the implementation of the Governance Framework. Critical observations shall be cleared before the stage 2.

In phase 2, about Section B, Governance of controls (policies and main procedures) will be audited before to verify the implementation of controls that are in Phase 3, during stage 2.

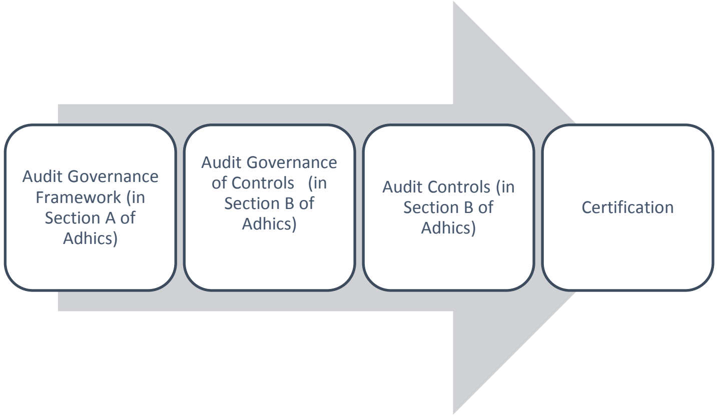

Audit Governance Framework (in Section A of Adhics)
Audit Governance of Controls (in Section B of Adhics)
Audit Controls (in Section B of Adhics)
Certification

Figure – flow of audit flow

Certification will be granted only once audit will complete the stage 2 of verification of implementation of controls, otherwise a report will be release without achievement of status of certified.

Audit will be performed based on the principles of the ISO 19011:2018, by process approach and by sampling basis. Sampling is not intended as 'statistical', but following the 'judgement based sampling' (as per the A.6.2 of the ISO 19011:2018), partially depending from the outputs of the stage one audit, or previous years' audits, and from validations of self-assessment quarterly submissions (and e.g. from Facility Malaffi security assessment submissions).

Stage 1 Section A

Audit on Governance Framework - Phase 1

- check on Section A

Stage 1 Section B

Audit on Governance of controls (policies) - Phase 2

- from the 11 domains

Stage 2 Section B

Audit on Controls/Sub controls - Phase 3

- from the 11 domains

Evidence in documented or electronic means will be retained for a duration established for compliance monitoring from DoH. Evidence could be retained directly in the DoH repository systems. Requests of evidence of supporting documentation, and identified deviations, whatever they are collected to be retained or not, will respect the following:

i. Documents and or evidence of the implementation of the ADHICS system, will be uploaded in the audit tool/software. When above is not applicable, or additionally evidence is required, all the documents reviewed in electronic format will be directly collected as evidence by the auditors themselves. It shall be the responsibility of the auditee to hand over all the other required documentation and requested evidence before the auditor leaves on the scheduled day and time.

ii. Failure to provide the requested evidence within the 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.

iii. The Health Information Systems should have capability to electronic print/save the required visit documents as audit evidence. Not having the option or such feature to provide evidence shall be considered as no evidence provided and the auditor findings documented with specific reference remains valid.

iv. It is highly recommended to provide evidence in electronic format to save paper and time.

v. The evidence can be masked with confidential patient information, when applicable, retaining other required details of visit and other pertinent information, such as patient code or assigned id. number

vi. It is the responsibility of the auditee to provide all the evidence by documentations requested during the audit.

NOTE 1: It shall be the responsibility of the auditee to acquire all the approvals, if necessary, prior of sharing information and in any case, prior to start stage 1 or stage 2 audits.

NOTE 2: Any evidence missed from the list requested by the auditors will be a sole responsibility of the auditee and shall be considered as no available during our further reviews.

4 CORRECTIVE ACTION PLAN AND REPORT

Upon the completion of each of the audit stage, a copy of noncompliance points will be issued at the earliest.

In stage 2 Auditee is required to send the corrective action plan within 10 working days. More details in the next chapter.

A written full report will be delivered from TASNEEF to the authorized representative responsible for the auditee within 10 working days from the audit stage 2 completion. A report for stage 1 will be released also marking mainly the findings.

The report should be communicated to the CEO or CFO or COO or equivalent of delegated authority of the auditee from the Information Security Governance Committee.

After stage 2 audit, once corrective action plan (if applicable) from the auditee is approved, a certification file including those corrective actions and report, will be submitted for the review of a Certification Committee and for final decision from DoH.

The audit report is owned by DoH and it is confidential. Report shall not be shared externally for any reason or made public.

The auditee may indicate any comments concerning the findings by the TASNEEF auditors in the relative space in the audit report along with the corrective actions.

Considering the audit as Third-party concept, such comments from auditee cannot be as a dispute or on-going discussion. Auditee can express concerns or clarifications, or comments to the Lead auditors by email or by the platform, in regards of the audit report outcomes.

4.1 Audit Report Stage 2 Format

The Report will include, but will not be limited to:

- A Cover page with of profile of   Facility/ Entity/ Party Name and license when applicable.
- Executive Summary
- Narrative of the Audit (scope and exclusions, team, time, closure of previous findings, evaluations, recommendations, areas of improvements)
- Assessment Findings on level of compliance
- All circumstances if any, that have been verified and validated by TASNEEF
- Corrective Actions
- Planned date for next activity
- Risks identified
- 3 years' Audit program including planned dates and scope for surveillances and recertification

5 NON-COMPLIANCE AND CORRECTIVE ACTIONS

Auditee should respond to TASNEEF through the system of DoH with a definitive action plan to resolve the identified noncompliance and risks, within 10 working days from raising the noncompliance findings in stage 2. Any delay in sending the corrective action plan may delay decision. Such delays resulting in any gap, in any listing or any other impacts shall not be the responsibility of TASNEEF and may lead to failure of certification.

Each aspect of before mentioned domains for audit shall be verified for compliance to the requirements of the standard.

Adequacy of the ADHICS implementation will be verified through assessment questions, as per the table below.

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's 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.

Table of compliance findings – definitions

All the non-complaint findings must be rectified with a corrective action plan supported by root cause analysis. In all cases is very important to quickly implement those corrections to remove current risks in information. Here below explanatory definitions of corrections and corrective actions.

Correction is an action taken to eliminate a detected noncompliance. It will be essential to quickly remove any noncompliance when those are strongly affecting the information security or cybersecurity.

Corrective Action: Corrective actions are steps that are taken to eliminate the causes of existing noncompliance to prevent recurrence.

Corrective Action Plan: A step-by-step plan of action and schedule for correcting a process or area of non-compliance. Corrective action plan shall be submitted from auditee within 10 working days for each stage of audit from the issue of findings. The corrective action should provide information as to What is the non-Compliance, identified Root cause, what is the corrective action, who is responsible for the corrective action, when is the corrective action targeted to be completed.

As per the International standards and best practices, a target date of corrective actions to be implemented is set to be within a maximum of 90 days.

The Leadership of the organization should understand, acknowledge, and assume the responsibility to monitor the corrective actions and ensure the compliance.

Any disagreements documented in the corrective action plan are not considered as a corrective action. A proper corrective action is required to be submitted otherwise affecting the effective completion of audit process.

6 DECISION MAKING

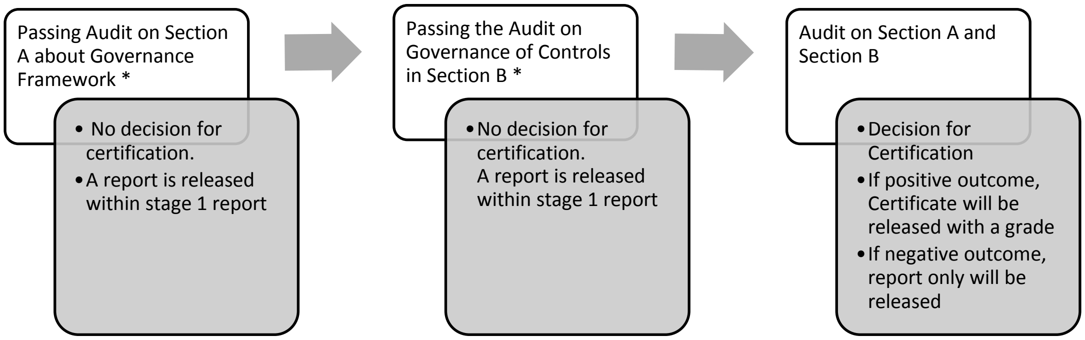
Decision is under the authority of DoH, made by a Technical Committee. Report and collected evidence will be part of a certification proposal with audit score details and corrective action plans. TASNEEF reserves the right to reject the corrective action plans if supposed to be not meeting the requirements of corrective actions and any disagreements on auditor findings. Auditee can request for more details to understand the non-compliance to provide the corrective action plan. Decision making could be supported from an Advisory Committee with selected experts from the industry.

Facilities will be graded based on the scores achieved. Certification will have a validity of three years.

For first year a grade will be assigned and confirmed or updated during the remaining two years 'validity.

Grade is confidential. Auditee can appeal on the audit results or grade by filing an appeal request to the related committee.

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 for 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

* In case of major findings during stage 1, those will be corrected before stage 2
**In Case of auditee is part of a group or a corporate or referred to a 'pivot' subject, where management of strategies and preparation and implementation of policies is centralized, the audit on Section A and Section B (for Governance of controls/ policies) must be conducted in the centralized function, but implementation and awareness of staff on the centralized policies shall be verified.

Here below the summary of the certification steps and the graph of the audit framework along with the flow of activities.

Step	Responsibility	Label of information
Kick off communication – Project start	TASNEEF - DOH	Restricted
Uploads of information	AUDITEE	Restricted
Audit plan stage 1	TASNEEF	Restricted
Upload of documentation	AUDITEE	Restricted
Desktop Audit Stage 1 – Review of documentation uploaded from auditee	TASNEEF	Restricted
Interviews stage 1	TASNEEF - AUDITEE	Restricted
Findings Stage 1	TASNEEF	Restricted
Audit Report Stage 1	TASNEEF	Restricted
Closure of findings Stage 1	AUDITEE	Restricted
Audit Plan Stage 2	TASNEEF	Restricted
Desktop audit (review of documentation uploaded from auditee) stage 2	TASNEEF - AUDITEE	Restricted
Interviews stage 2	TASNEEF - AUDITEE	Restricted
Noncompliance findings if any	TASNEEF	Restricted
Reporting Stage 2	TASNEEF	Confidential
Corrective actions plan	AUDITEE	Restricted
Corrective actions plan approval	TASNEEF	Restricted
Three years surveillance program	TASNEEF	Restricted
Decision (if positive)	TASNEEF	Confidential
Certificate with Grade	TASNEEF	Confidential
Decision (if negative)	TASNEEF	Confidential
Re audit	TASNEEF- AUDITEE	Restricted
Decision with Grade	TASNEEF	Confidential

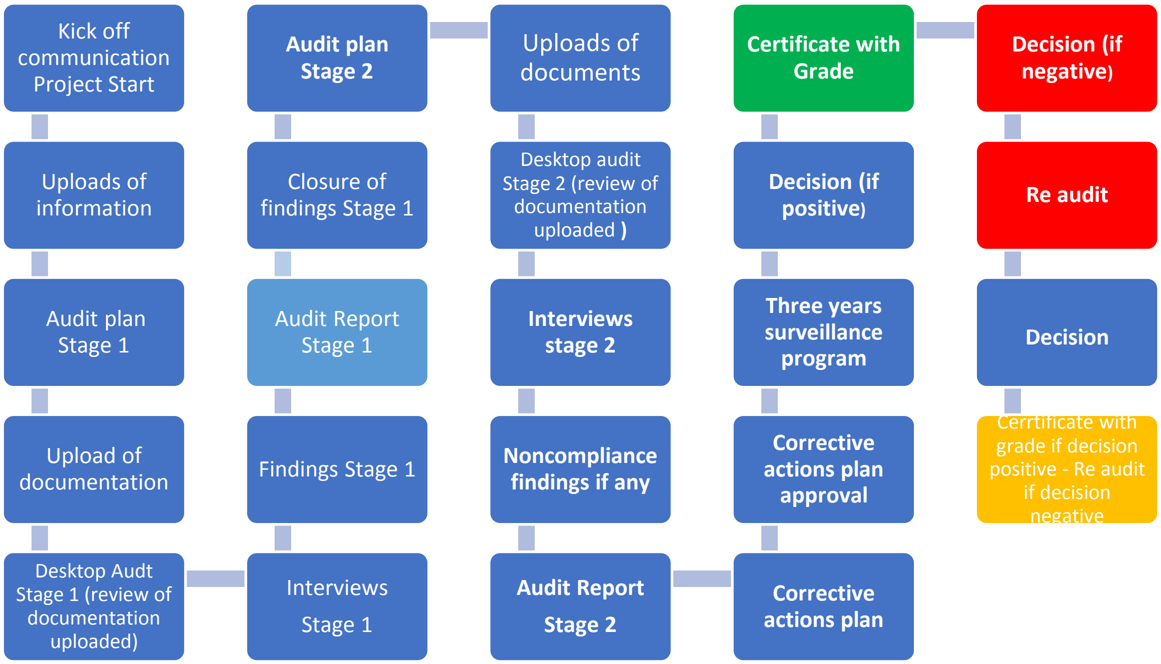

Kick off communication Project Start
Uploads of information
Audit plan Stage 1
Upload of documentation
Desktop Audt Stage 1 (review of documentation uploaded)
Interviews Stage 1
Findings Stage 1
Audit Report Stage 1
Closure of findings Stage 1
Audit plan Stage 2
Uploads of documents
Desktop audit Stage 2 (review of documentation uploaded)
Interviews stage 2
Noncompliance findings if any
Audit Report Stage 2
Corrective actions plan
Corrective actions plan approval
Three years surveillance program
Decision (if positive)
Certificate with Grade
Decision (if negative)
Re audit
Decision
Cerrtificate with grade if decision positive - Re audit if decision negative

Table for the flow of audit and certification activities.

7 CERTIFICATION SCORE AND GRADE SYSTEM FOR ADHICS DATA CERTIFICATION

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

For groups of entities, the score will be unified considering aggregated or unified (see example in Appendix 1).

Score is made by the average of the score in each of the eleven domains of ADHICS, as resulting from the stage 2. In each domain the score is the outcome only of controls checked. Controls not checked will not be considered neither positive nor negative. For example, if in one domain 10 questions are checked, only those 10 questions will generate the score for that domain. The average of all 11 domains score will be generating the final score and grade. A presence of many non-compliant basic controls, fully not met, it is configuring a scenario of major concern from DoH.

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

Table of scores

7.1.1 Non-certifiable

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

Table of Maturity level

7.1.2 Impact of the audits

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.

8 RE-AUDITS AND AD HOC AUDITS

Failing certification audit will be in general having consequence to repeat the audit in the area of noncompliance. That means in case of serious concerns from DoH on certain domains of audit and as per the result in score very less than 86 with many non-compliant findings , 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. * Applicability of fee charge will be defined by a Circular or information from DoH relevant departments.

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

9 CERTIFICATE

- The issuing of certifications is a responsibility of TASNEEF and DOH based on Certification Committee decision.
- Certificate is not a public information, and grade is anyway confidential, however Certificate identification number (cert. id. N) can be shared to certain interested parties (for example a consultant certified can provide the cert. id. N to a hospital, to enable the hospital to verify with DoH on validity of the certificate).
- 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.)

- DoH retains the right to revoke certification based on substantive evidence that the audit of this facility was not representing the real system in place. Revocation is also applicable in case there is evidence of improper conduct which may include but is not limited to:
  - Evidence of documentation manipulation
  - Evidence of bribery or collusion
  - Major cybersecurity or information security incident

10 TRANSITION PHASE

Certification will be applied annually to certain facilities/ entities and parties identified by DoH in specific batches, even though the ADHICS standard shall be implemented by all identified entities as per the standard's specifications.

ADHICS Standard might be revised, and in such cases, Certification will follow the new revision only when formally published and implementation of new requirements shall be integrated from the auditee, as per the timelines defined by DoH.

11 MAINTAINING VALIDITY OF THE CERTIFICATE

Auditee must ensure its System continues to comply with the Standard. The facility must record any complaints / claims/incident and the relative corrective action implemented and must make these records available together with the corrective action taken to address the identified deviations.

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.

11.1 Management of Certificates

1. The validity of the certificate is of three years from date of initial decision. The validity of the certificate may be suspended and withdrawn.
2. 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.
3. The grade in the certificate, could be modified as per the scores of the surveillance audits.

12 MODIFICATION OF CERTIFICATION AND COMMUNICATION OF CHANGES

1. The facility/ entity/ party must promptly inform TASNEEF of any changes in factors that may affect the capacity of the Management System to continue to satisfy the requirements of ADHICS
2. These requirements concern, for example, modifications to the legal, commercial or ownership status.
3. TASNEEF reserves the right to perform additional audits if the modifications communicated are considered particularly significant in regards of maintaining the compliance of the Management System and Controls and to review the economic conditions for the possible modification of the contract, when applicable. Such audits shall not exceed 2-man days.

4. TASNEEF and DoH will promptly informed, whenever any changes in the methodology, reference standards or certification rules are going to be applied.

13 CONDITIONS AT WHICH AUDIT PROCESS WILL STOP

1. When in the assessment of Section A or B, number of non-compliant findings are showing clarity on absence of a management system and controls in place.
2. When required evidence of compliance is not provided on time.
3. When the planned nominated personnel are not available and or the not competent to provide support.
4. Absence of authorized person from the top management to facilitate the audit process.
5. Any case that might be classified by the lead auditor as a reason such as:
    i. Unavailable agreed resources
    ii. Unavailability of required employees
    iii. 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.
6. 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

14 CONDITIONS AT WHICH CERTIFICATION PROCESS MAY BE SUSPENDED

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

15 SUSPENSION, REINSTATEMENT AND WITHDRAWAL OF CERTIFICATION

The validity of the certificate of compliance may be suspended in the following specific cases:

- 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 the other reason mentioned in these rules;

This suspension will be notified in writing, stating the conditions for re-instating certification and the date by which the new conditions are to be complied with.

Revocation of the certificate may be decided in the following specific cases:

- 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

Withdrawal of the Certificate is notified in writing to the Facility/ Entity/ Party.

Following revocation of its Certificate, auditee must restart by a new certification and follow the entire procedure all over again.

16 RENUNCIATION OF CERTIFICATION

A certified facility/ entity/ party may send formal communication of renunciation of certification to TASNEEF in case of business termination before the expiry of the certificate, if allowed by DoH regulations.

Upon receipt of this communication, TASNEEF starts the procedure for invalidating the Certificate after a decision from the certification committee. Within one month from the date of the communication, TASNEEF updates the validity status of the certificate.

17 COMPLAINTS MANAGEMENT

TASNEEF and DoH have always considered complaints and customer satisfaction as an incentive to improve the quality of the service provided. This chapter describes how third and interested parties can file a complaint with certification concerning its activities. All the complaints should be sent to the dedicated channel in TASNEEF website and they will be responded by email from ba.technical@tasneef.ae and cc adhics@doh.gov.ae. Complaints routed through this email will be responded as per the complaint's management procedure involving also DoH and to the attention to a dedicated committee. The communication must include all the data enabling TASNEEF activity for which a complaint is being filed to be identified. The specific aspect of complaint for review will be identified, and a receipt notification will be sent to the facility within 10 working days describing the request management process.

As per reporting process:

1. All the audit findings are communicated to the facilities and represented also in the audit report.
2. Any appeal request shall include the auditee license, region, head details and the Audit representative details along with the information of audit concerns with supporting documents and references.
3. Complaints/Feedback tab is available on the webpage of TASNEEF at http://www.tasneefba.ae/content/public-information or at 'ba.technical@tasneef.ae', addition to reporting the same to DOH at 'adhics@doh.gov.ae'

APPENDIX-I

Scoring Example
Scoring

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%

HIE 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	a
56 - 75 %	Defined	
76 - 90 %	Managed	Grade C =>86-89%
91 - 100 %	Optimized	Grade B=>90-95% Grade A=>96-100%