الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) Audit Accreditation Standard

[NCSA-NISCF-ACCR-AUD-NIA-STND]

Requirements for Accreditation of NIA Audit Service Providers

National Cyber Security Agency (NCSA)

October 2024

V2.0

C0 – Public / PS1 – Non-Personal Data (Non-PD)

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Document Control

Document Details	
Document ID	NCSA-NISCF-ACCR-AUD-NIA-STND
Version	V2.0
Classification & Type	C0 – Public / PS1 – Non-Personal Data (Non-PD)

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this publication, titled "National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) Audit Accreditation Standard" - V2.0 - C0 – Public / PS1 – Non-Personal Data (Non-PD), in order to provide the requirements for applicants to NIA Audit Accreditation Service, NIA Accredited Audit Service Providers and for the delivery of NIA audits.

NCSA is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge NCSA as the source and owner of the "National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) Audit Accreditation Standard".

Any reproduction concerning this document with the intent of commercialization shall seek a written authorization from the NCSA. NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

The assurance provided is not absolute and its based-on documents and information shared by the Service Providers and based on an assessment performed at a particular point in time. Therefore, NCSA does not hold responsibility of errors, damages or losses resulting from the usage of products or consumption of services provided by Accredited Service Providers.

LEGAL MANDATE(S)

Based on Emiri Decree No 1 of year 2021, National Cyber Security Agency (NCSA) – National Cyber Governance and Cyber Assurance Affairs (NCGAA) is the entity responsible for issuing certificates for Technology and Information Security service providers and Certificates of Compliance with National Information Security standards and policies.

This standard has been prepared to take into consideration the current applicable laws of the State of Qatar. If a conflict arises between this document and the laws of Qatar, the latter shall take precedence. Any such term shall, to that extent be omitted from this document, and the rest of the document shall stand without affecting the remaining provisions. Amendments, in that case, shall then be required to ensure conformance with the relevant applicable laws of the State of Qatar.

Table of Contents

1. Introduction

The National Information Security Compliance Framework (NISCF) helps to support the achievement of Qatar's National Cyber Security Strategy; it complements Qatar's National Information Assurance Framework (including wider applicable information security legislation, regulation, and standards) to establish safe and vibrant cyberspace.

NCSA offers NIA Audit Accreditation Service for Service Providers that are willing to participate in the delivery of NIA Audits related to NIA Certification Service.

Service Providers shall comply with the requirements defined in this standard and other related specific requirements published by NCSA in relation to NIA Certification audits, to obtain the NIA Accreditation and ongoing maintenance.

NIA audits during NIA Certification processes can only be performed by NIA Audit Accredited Service Providers or NCSA.

2. Purpose and Scope

2.1. Purpose

The purpose of this document is to provide requirements for organization willing to request for NIA Audit Accreditation Service, NIA Accredited Audit Service Providers and for the delivery of NIA audits.

2.2. Scope

This document applies to all applicants to the NIA Audit Accreditation Service, NIA Accredited Audit Service Providers and the audits they deliver related to the NIA Certification service.

3. Key Definitions

The terminologies used in this document are consistent with the definitions provided in the NCSA-NISCF-ACCR-GTXD (General Taxonomy Document for National Accreditation - Public), NCSA-NISCF-AUD-STND (NISCF Audit Standard - Public), NCSA-NISCF-AUD-STND (NISCF Audit Standard) and NCSA-NISCF-CERT-NIA-SS (NIA Certification Scoping Standard).

4. Standard Requirements

G. Governance

G.1. Organizational Environment, Monitoring, Quality & Review

G.1.1. Legal Entity

G.1.1.1. The Service Provider shall provide a valid company registration certificate, in accordance with applicable laws in the State of Qatar.

G.1.2. Audited Financial Statement

G.1.2.1. The Service Provider shall provide the latest audited Financial Statements that shall contain an unmodified opinion.

G.1.3. Liability & Insurance

G.1.3.1. The Service Provider shall provide evidence of annual insurance coverage (Professional Indemnity and Cyber Insurance) covering least its audit Service offering (including Cyber Security audit). The Service Provider shall provide a written and approved justification of the coverage amount.

G.1.4. Organizational Structure with, Duties, Responsibilities, and Authorities of Management

G.1.4.1. The Service Provider shall provide a documented organizational structure with clear identification of the department under which the National Information Assurance (NIA) audit service is operating and the related roles.

G.1.4.2. The Service Provider shall provide documented job descriptions of the different roles in the Service Provider's NIA audit team.

G.1.4.3. The Service Provider shall provide documented evidence clearly identifying the person, unit, or committee having the ultimate authority for the approval of policies, processes, procedures, methodologies related to the operation of the NIA audit service.

G.2. Principles, Policies & Processes

G.2.1. Personnel Management Process

G.2.1.1. The Service Provider shall provide its Personnel Management Process, which shall be used for the hiring and evaluation of the Service Provider's NIA audit team, and that shall include:

- A process for hiring personnel, as part of the Service Provider's NIA audit team, that shall include a competencies assessment step; and
- A process for ongoing competencies monitoring of personnel involved in the delivery of the NIA audit service, at least once in every calendar year (Annually), based on competencies criteria and performance evaluation (please refer to requirement **G.2.1.2**).

G.2.1.2. The Service Provider shall provide evidence that performance evaluations include on-site performance evaluation, review of audit work and feedback from clients.

G.2.1.3. The Service Provider shall provide evidence of a forecasting and project assignment process of the Service Provider's NIA audit team that shall be used for the capacity and capability management of the Service Provider's NIA audit team and its allocation.

NOTE: This process and its application shall allow the Service Provider to ensure it employs and / or has access to a sufficient number of Auditors, including Lead Auditors, Engagement Leads and Technical Experts.

G.2.1.4. The Service Provider shall provide evidence of the process used for selecting and authorizing audit team members, to be involved in NIA audit engagements: This process shall align with:

- Requirements A.P.2.2.5. Audit Team Selection of the NISCF Audit Standard; and
- Steps SOP-ATS-ISAT-(01-06) from NIA Audit Team Selection Standard Operating Procedure (NCSA-NISCF-ACCR-AUD-NIA-SOP-ATS).

G.2.2. Outsourcing

G.2.2.1. The Service Provider shall provide a documented outsourcing process of personnel as a part of the Service Provider's NIA audit team that shall cover or refer to:

- The risk management to identify, evaluate, mitigate, and monitor risks associated with procuring outsourced auditors;
- The vetting of the outsourced personnel in conformance with the process provided in reference to requirement **G.3.3.1**; and

- The competencies evaluation of the outsourced personnel in conformance with requirement **G.3.1.1**.

NOTE: Interfirm outsourcing or the use of an individual or employee of another legal entity, individually contracted or otherwise, to take part in the delivery of the NIA audit service, does constitute outsourcing. If the Service Provider does not use third parties, the Service Provider shall provide evidence in the form of an approved written policy or official communication from an authorized person formally stating the prohibition of outsourcing.

G.2.2.2. The Service Provider shall have a standard legal agreement by which the outsourced personnel commit to comply with the Service Provider's applicable policies, processes, and procedures related to the NIA audit activities. The agreement shall address confidentiality and impartiality safeguards and compliance with personal data protection requirements, in accordance with State of Qatar Laws and Regulations.

NOTE: In cases where a policy document is used to outline the above obligations, the agreement shall reference and acknowledge the provisions stated in the policy and the policy shall be provided.

G.2.3. Impartiality

G.2.3.1. The Service Provider shall provide a process for monitoring, identifying, assessing & mitigating conflicts of interest risks related to NIA audit engagements. This process shall account for and consider the requirements defined in section A.C.E.2.3.1. Impartiality and Independence of the NISCF Audit Standard.

G.2.3.2. The Service Provider shall have documented top management commitment to impartiality for NIA audit service. The documentation shall include the following key elements:

- Statement of Impartiality;
- Impartiality Policy; and
- Responsibilities and Roles.

G.3. People, Skills, and Competencies

G.3.1. Personnel Record and Evaluation

G.3.1.1. The Service Provider shall provide the Personnel Record Form for all personnel in the Service Provider's NIA audit team (including outsourced personnel) that:

- Constitutes the exhaustivity of the Service Provider's NIA audit team and will be the only reference in the Accreditation as of the allowed personnel to participate in NIA audit engagements;
- Evidence competency evaluation (against the defined in section 6.2 Service Provider's NIA Audit Team Competencies Requirements); and
- Documents the personnel commitment to the Code of Ethics and Professional Conduct defined in section A.C.E.2.3. Code of Ethics and Professional Conduct of the NISCF Audit Standard.

Note: Post-Accreditation the Personnel Record Form shall be updated annually as part of the ongoing competencies monitoring (please refer to requirement **G.2.1.1**) and recorded for new personnel enrolled in the Service Provider's NIA audit team (please refer to requirement **G.2.1.1**) and submitted during each Maintenance.

G.3.2. Knowledge Management

G.3.2.1. The Service Provider shall provide an annual training plan for all the personnel of the Service Provider's NIA audit team.

Note: The training selection shall be justified through needs or gaps in competencies (please refer to requirement **G.3.1.1**) following the Service Provider's needs, ongoing monitoring of competencies and performance.

G.3.3. Personnel Requirements

G.3.3.1. The Service Provider shall provide a documented process for vetting of the Service Provider's NIA audit team, and the supporting evidence that is has been applied for all personnel, that shall include at least:

- Verification of employment history and qualifications;
- Ethical misconduct; and
- Past criminal convictions.

G.3.3.2. The Service Provider shall maintain as part of the Service Provider's NIA audit team at all times:

- At minimum one (1) Engagement Lead[1];
- At minimum one (1) NIA Lead Auditor; and
- At minimum three (3) NIA Auditors.

G.3.3.3. The Service Provider shall ensure that all Lead Auditors and Auditors as part of its NIA audit team hold "NIA Certified Auditor" Credential from NCSA.

G.4. Culture, Ethics & Behavior

G.4.1. Code of Ethics and Professional Conduct

G.4.1.1. The Service Provider holds individuals accountable for their responsibilities and shall ensure that the NISCF Audit Standard Code of Ethics and Professional Conduct (please refer to section s A.C.E.2.3. Code of Ethics and Professional Conduct of the NISCF Audit Standard) is acknowledged by each personnel part of the Service Provider's NIA audit team (please refer to requirement **G.3.1.1**).

G.4.1.2. The Service provider shall have a process to perform periodic related refreshes and reminders for audit ethics principles aligned with the NISCF Audit Standard Code of Ethics and Professional Conduct.

[1] In accordance with the NISCF Accreditation Terms and Conditions, the Engagement Lead shall not be outsourced.

M. Management

M.1. Security and Risk Management

M.1.1. Compliance and Security Requirements

M.1.1.1. The Service Provider shall have documented and approved information security policies and procedures[2] covering:

- Information Assets Management;
- Confidentiality and Acceptable Use;
- Identity and Access Management;
- Incident Management;
- Third-party Security Management; and
- Physical Security.

M.1.1.2. The Service Provider shall have a valid National Information Assurance (NIA) Certification covering the NIA audit activities.

Note: ISO / IEC 27001 valid Certification from a Certification Body recognized by the International Accreditation Forum (IAF) covering the scope, is acceptable, if a commitment is provided to achieve NIA Certification within 3 years.

M.1.1.3. The Service Provider shall provide a documented process to retain and archive in a secure, encrypted, and redacted format all audit documentation, that shall be used in all NIA audit engagements.

M.1.1.4. The Service Provider shall provide a retention policy and records retention register for the audit documentation referred to in requirement **M.1.1.3**, for a minimum retention period of five (5) years after completion of an NIA audit engagement and a maximum retention period of three (3) years after the end of the relationship with the client.

[2] National Information Assurance (NIA) Standard can be used as reference to develop the required policies and procedures.

M.1.2. Tools & Systems

M.1.2.1. The Service Provider shall provide the list of systems it uses to perform audit activities as mentioned in section A.C.E.3. Audit Technology and requirement A.P.1.2.1.2 of the NISCF Audit Standard.

M.2. Project and Continuity Management

M.2.1. Project Management

M.2.1.1. The Service Provider shall provide a documented process and artifacts for managing risks and issues during NIA audits, including situations mentioned in requirements A.C.E.1.5.1.4, A.C.E.2.3.1.9 and A.C.E.2.3.1.10 of the NISCF Audit Standard and other supporting Standard Operating Procedures (SOP) and Technical Directives (TD) that require escalation to the client and / or NCSA (please refer to section A.P.4.4 of the NISCF Audit Standard).

M.2.1.2. The Service Provider shall provide evidence of mechanisms in place to prevent audit team members from beaching Intellectual Property (IP) of evidence they gain access to.

M.2.2. Segregation of Duties (SoD)

M.2.2.1. The Service Provider shall provide a documented Segregation of Duties (SoD) matrix for the NIA audit activities defined in this standard (please refer to section **S. Service (NIA Audit)**), based on the key audit roles (please refer to section A.C.E.2.1. Key Audit Roles of the NISCF Audit Standard) that shall allow to implement the four (4) eyes principle.

M.2.3. Continuity Management

M.2.3.1. The Service Provider shall provide a documented process and artifacts by which it manages resource limitations and constraints to allow to complete audit engagements as per the defined timeline in NISCF Audit Standard and other supporting Standard Operating Procedures (SOP) and Technical Directives (TD).

S. Service (NIA Audit)

S.1. Client / Engagement Acceptance

S.1.1. Engagement / Client Acceptance Due Diligence and Relationship Continuance Confirmation

S.1.1.1. The Service Provider shall provide a documented process for conducting the engagement / client acceptance due diligence, that shall be used in NIA audit engagements, and that shall conform with the requirements defined in sections A.P.1.1. Engagement / Client Acceptance Due Diligence and A.P.1.5. Relationship Continuance and Monitoring of the NISCF Audit Standard.

S.1.1.2. The Service Provider shall provide tools and templates for conducting the engagement / client acceptance due diligence, based on the process referred to in requirement S.1.1.1, that shall be used in NIA audit engagements, and that shall conform with the requirements defined in sections A.P.1.1. Engagement / Client Acceptance Due Diligence and A.P.1.5. Relationship Continuance and Monitoring of the NISCF Audit Standard.

S.1.2. Engagement Documentation

S.1.2.1. The Service Provider shall provide a Non-Disclosure Agreement (NDA) template, which shall be used in NIA audit engagements with its client, and that shall enforce:

- Confidentiality obligations of client's information obtained or created during the NIA audit to all employees, outsourced resources, and other individuals acting on the Service Provider's behalf;
- Not sharing information about the client, the audit and related individuals to a third party (except NCSA) without the written consent of the client or individual concerned;
- Notification of the client of the information related to the audit shared with NCSA; and
- Notification in advance of the client's confidential information release to a third party when required by law, unless the notification is regulated by law.

S.1.2.2. The Service Provider shall provide a template of a legally enforceable agreement, that serves as a contract between the Service Provider and its clients, that shall be used in NIA audit engagements, and that shall conform with the requirement A.P.1.3.1.1 of the NISCF Audit Standard.

S.2. Planning

S.2.1. Preliminary Work

S.2.1.1. The Service Provider shall provide working papers templates for recording the audit objectives, assertions, period, and criteria, that shall be used in NIA audit engagements, and that shall conform with the requirement A.P.2.1.1. Audit Objectives, Assertions, Period and Criteria of the NISCF Audit Standard and the specific Technical Directives (TD) for NIA audit(s) objectives(s) and scope(s) and NIA audit period.

S.2.1.2. The Service Provider shall provide working papers templates for recording and updating the understanding of the organization(s) subject of the audit and the audit environment, that shall be used in NIA audit engagements, and that shall conform with the requirements defined in section A.P.2.1.2. Environment Understanding of the NISCF Audit Standard.

S.2.1.3. The Service Provider shall provide working papers templates for reviewing and confirming the scope, that shall be used in NIA audit engagements, and that shall conform with the requirements defined in section A.P.2.1.3. Scope Review and Confirmation of the NISCF Audit Standard and the specific Technical Directives (TD) for NIA audit(s) objectives (s) and scope(s).

S.2.2. Planning

S.2.2.1. The Service Provider shall provide working papers templates used for recording the audit risk assessment conducted, that shall be used in NIA audit engagements, and that shall conform with the requirements defined in section A.P.2.2.1. Audit Risk of the NISCF Audit Standard and the specific Standard Operating Procedures (SOP) for NIA audit risk.

S.2.2.2. The Service Provider shall provide a documented standard audit work program that shall cover all the requirements defined in the NIA Standard, all audit activities as per the NISCF Audit Standard and other supporting Standard Operating Procedures (SOP), and all NIA Certification lifecycle, that shall be used and tailored, if necessary, in NIA audit engagements, and that shall conform with the requirements defined in section A.P.2.2.2. Audit Work Program of the NISCF Audit

Standard and the specific Standard Operating Procedures (SOP) for NIA audit work program.

S.2.2.3. The Service Provider shall provide working papers templates for performing sampling, that shall be used in NIA audit engagements, and that shall conform with the requirements defined in section A.P.2.2.3. Audit Sampling of the NISCF Audit Standard and the specific Standard Operating Procedures (SOP) for NIA audit sampling.

S.2.2.4. The Service Provider shall provide working papers templates to document, justify, and review the use of work of others performed outside of the context of the audit (i.e., performed by other experts outside of the boundaries of the NIA audit), that shall be used in NIA audit engagements, and that shall conform with the requirements defined in section A.P.2.2.4. Use of the Work of Others of the NISCF Audit Standard and the specific Technical Directives (TD) for usage of work of others in NIA audit(s).

S.2.2.5. The Service Provider shall provide working papers templates for recording audit team members selection and activities assignment, that shall be used in NIA audit engagements, and that shall conform with the requirements defined in section A.P.2.2.5. Audit Team Selection of the NISCF Audit Standard and the specific Standard Operating Procedures (SOP) for NIA audit team selection.

S.2.2.6. The Service Provider shall provide a documented procedure for determining the audit calendar, that shall be used in NIA audit engagements, and that shall conform with the requirements defined in section A.P.2.2.6. Audit Calendar of the NISCF Audit Standard and the specific Technical Directives (TD) for NIA audit calendar.

S.2.2.7. The Service Provider shall provide working papers templates for recording the audit calendar and its justification, based on the procedure referred to in requirement S.2.2.6, that shall be used in NIA audit engagements.

S.2.2.8. The Service Provider shall provide audit plan templates that shall be used in NIA audit engagements, and that shall conform with the requirements defined in section A.P.2.3. Plan Documentation of the NISCF Audit Standard.

S.3. Execution and Supervision

S.3.1. Audit Activities Performance

S.3.1.1. The Service Provider shall provide working papers templates to conduct and record the kick-off meeting, which shall be used in NIA audit engagements, and that shall conform with the requirements defined in section A.P.3.1.1. Kick-Off of the NISCF Audit Standard.

S.3.1.2. The Service Provider shall provide standardized testing working papers to record the performance and review of audit activities, that shall be used in NIA audit engagements, and that shall conform with requirements defined in sections A.P.3.1.3. Audit Documentation, A.P.3.1.4. Design Effectiveness (DE) Audit, A.P.3.1.5. Operating Effectiveness (OE) Audit and A.P.3.1.6. Findings and Conclusions of the NISCF Audit Standard and the specific Technical Directives (TD) for NIA Corrective Actions Plan (CAP).

S.3.2. Audit Supervision

S.3.2.1. The Service Provider shall provide working papers templates to track, assess, and record the audit progress and, that shall be used in NIA audit engagements, and that shall conform with requirements defined in section A.P.3.2.1. Monitoring and Adjustments of the NISCF Audit Standard.

S.4. Reporting and Completion

S.4.1. Completion

S.4.1.1. The Service Provider shall provide working papers templates to conduct and record the completion meeting, that shall be used in NIA audit engagements, and that shall conform with the requirements defined in section A.P.4.2. Completion of the NISCF Audit Standard.

S.4.2. Final Reporting

S.4.2.1. The Service Provider shall provide template of audit report, that shall be used in NIA audit engagements, and that shall conform with the requirement A.P.4.3.1.4. of the NISCF Audit Standard.

S.4.3. Other Reporting

S.4.3.1. The Service Provider shall provide working papers templates to record and report on the various potential situations described in section A.P.4.4. Other Reporting of the NISCF Audit Standard, that shall be used in NIA audit engagements, mainly:

- Timely response to specific Clarification and Evidence Request(s) from NCSA;
- Inability to obtain appropriate and sufficient audit evidence and unmanageable audit risk; and
- Changes impacting the scope.

S.5. Change (substitute) of Accredited Service Provider for NIA Audit

S.5.1. Auditors Transition Procedure

S.5.1.1. The Service Provider shall establish and maintain documented procedures for the transition of responsibilities from the previous Accredited Service Provider for NIA Audit to ensure continuity and consistency in NIA audit engagements. These procedures shall include the provision of necessary information and documentation as required by relevant Accreditation standard, processes, the NISCF Audit Standard and other supporting Standard Operating Procedures (SOP), Technical Directives (TD) and regulatory requirements.

5. Compliance and Enforcement

5.1. Compliance Process

All stakeholders to the NISCF Certification Services shall conform with the requirements defined in this standard.

5.2. Roles and Responsibilities

National Cyber Governance and Assurance Affairs (NCGAA) is responsible for enforcing and monitoring conformance to this standard.

5.3. Transitioning and effective date

5.3.1. Effective date

This standard is effective from January 1, 2025.

5.3.2. Transition period

Existing Accredited Audit Service Providers at the time of the publication of this standard shall make the necessary updates to conform with this standard before January 1, 2025.

Any new request for NISCF Audit Accreditation shall be in conformance with this standard from the date of publication.

5.4. Exceptions and deviations

5.4.1. Exceptions to Policy Statements

Exceptions to this standard shall only be defined by the National Cyber Security Agency (NCSA) through another policy or standard and / or any NCSA's organizational structure that has been given the authority over the NISCF or the Accreditation Services.

5.4.2. Deviation process from Policy Statements

Deviation from standard requirement shall be formally authorized in written by the National Cyber Security Agency (NCSA).

5.4.3. Sanctions

National Cyber Security Agency (NCSA) reserves the right to not accept NISCF Accreditation Services requests and / or suspend or withdraw Certificates of Accreditation or any other Certificates, Credentials or Licenses provided by NCSA from applicants to NISCF's Penetration Testing Accreditation Services and Accredited Penetration Testing Service Providers that do not conform with the requirements defined in this Standard.

National Cyber Security Agency (NCSA) reserves the right to impose any monetary or procedural sanctions in virtue of the authority that has been granted to NCSA, through laws and regulations.

6. Annexes

6.1. Acronyms

CAP	Corrective Actions Plan.
DE	Design Effectiveness.
IAF	International Accreditation Forum.
IEC	International Electrotechnical Commission.
ISO	International Organization for Standardization.
NC	Non-Conformities.
NCGAA	National Cyber Governance and Assurance Affairs.
NCSA	National Cyber Security Agency.
NDA	Non-Disclosure Agreement.
NIA	National Information Assurance.
NISCF	National Information Security Compliance Framework.
OE	Operating Effectiveness.
SoD	Segregation of Duties.
SOP	Standard Operating Procedure.
TD	Technical Directive.

6.2. Service Provider’s NIA Audit Team Competencies Requirements

The competencies criteria specify the knowledge and skills that the Service Provider’s NIA audit team shall have for each role in the NIA Audit Accreditation Service. The Service Provider shall evaluate its NIA audit team based on the competencies criteria defined in Annex 6.2. Audit Team Competence Requirement of the NISCF Audit Standard and the complementary competency criteria defined in this Appendix.

Required Competency		**NIA Audit Team Roles**		
Reference	**Knowledge and Skills**	**Engagement Lead**	**Lead Auditor**	**Auditor**
General				
C.AUD.NIA.G.1	Knowledge of NIA Certification standard and processes	X	X	X
C.AUD.NIA.G.2	Knowledge of NIA Certification timelines	X	X	
C.AUD.NIA.G.3	Knowledge of specific NIA Certification confidentiality requirements	X	X	X
C.AUD.NIA.G.4	Knowledge of NIA Certification retention requirements	X	X	
Service Delivery: Audit Service				
C.AUD.NIA.SD.1	Knowledge of NIA Certification audit(s) objectives and scopes	X	X	X
C.AUD.NIA.SD.2	Knowledge of NIA Certification audit(s) assertions	X	X	
C.AUD.NIA.SD.3	Knowledge of NIA Certification audit(s) period(s)	X	X	X
C.AUD.NIA.SD.4	Knowledge of the NISCF Audit Standard	X	X	X

Required Competency		NIA Audit Team Roles		
Reference	**Knowledge and Skills**	**Engagement Lead**	**Lead Auditor**	**Auditor**
C.AUD.NIA.SD.5	Knowledge of the Service Provider's tools, templates and working papers for NIA Certification audit(s)	X	X	X
C.AUD.NIA.SD.6	Knowledge of the Service Provider's systems, procedures and methodologies for NIA Certification audit(s)	X	X	X
C.AUD.NIA.SD.7	Knowledge of the Service Provider's audit work program for NIA Certification audit(s)	X	X	X
C.AUD.NIA.SD.8	Knowledge of the mapping and gaps between NIA requirements and national and / or international standards and framework requirements	X	X	X
C.AUD.NIA.SD.9	Knowledge of NIA audit risk assessment procedure	X	X	
C.AUD.NIA.SD.10	Knowledge of NIA sampling procedure		X	X
C.AUD.NIA.SD.11	Knowledge of NIA audit work program development procedure		X	
C.AUD.NIA.SD.12	Knowledge of the NIA audit criteria	X	X	X
C.AUD.NIA.SD.13	Knowledge of NIA audit team selection procedure	X	X	
C.AUD.NIA.SD.14	Knowledge of NIA audit calendar requirements	X	X	
C.AUD.NIA.SD.15	Knowledge of NIA Corrective Actions Plan (CAP) audit requirements		X	X
C.AUD.NIA.SD.16	NIA requirements auditing skills		X	X

6.3. Reference

Emiri Decree No 1 of year 2021

President of National Cyber Security Agency (NCSA) Decision No 3 of year 2022

NCSA-NISCF-CERT-GTXD (General Taxonomy Document for National Certification - Public)

NCSA-NISCF-ACCR-GTXD (General Taxonomy Document for National Accreditation - Public)

NCSA-NISCF-ACCR-GPNA (General Policy for National Accreditation - Public)

NCSA-NISCF-CERT-GPNC (General Policy for National Certification - Public)

NCSA-NISCF-CERT-SMSC (Standard for Management Systems Certification - Public)

NCSA-NISCF-ACCR-SNA (Standard for National Accreditation - Public)

NCSA-NISCF-AUD-STND (NISCF Audit Standard - Public)

NCSA-NISCF-CERT-NIA-SS (NIA Certification Scoping Standard - Public)

End of Document