الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) – Audit(s) Objectives and Scopes

[NCSA-NISCF-NIA-TD-AOS-001]

Technical Directive

National Cyber Security Agency (NCSA)

October 2024

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

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Document Control

Document Details	
Document ID	NCSA-NISCF-NIA-TD-AOS-001
Classification & Type	C0 – Public / PS1 – Non-Personal Data (Non-PD)

DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this Technical Directive, titled "National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) – Audit(s) Objectives and Scopes – Technical Directive" - C0 – Public / PS1 – Non-Personal Data (Non-PD), in order to provide the specific rules and recommended guidelines to be observed by the Accredited Audit Service Providers and NIA Certification Service Applicant / NIA Certification subject (auditee) during NIA Certification Audits, in relation to audit(s) objectives and scopes, as part of National Information Security Compliance Framework (NISCF) Certification Services of the National Cyber Security Agency (NCSA).

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(s) Objectives and Scopes".

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.

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 document 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 compliance with the relevant applicable laws of the State of Qatar.

Table of Contents

Table of Figures

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 Audit Service Accreditation for Service Providers that are willing to participate in the delivery of audits related to NISCF's Services.

National Information Assurance (NIA) Certification is one of the NISCF's services that requires the reliance on Audit Service Providers.

Accredited Audit Service Providers shall comply with the rules defined in this document when performing NIA Certification Audit. Conformance to this directive is considered in the maintenance of the Audit Service Providers Accreditation.

NIA Certification Service Applicant, NIA Certified Organizations and NIA Certification Subject (auditee) shall comply with the rules defined in this document when performing NIA Certification Audit. Conformance to this directive, by the NIA Certification Service Applicant, NIA Certified Organizations and NIA Certification Subject (auditee) is considered in the acceptance / rejection of a NIA Certification Application, grant / denial of NIA Certificate of Compliance, its maintenance, expansion and renewal.

2. Purpose and Scope

2.1. Purpose

This Technical Directive has been developed with the objective to provide specific technical rules to be followed and recommendations to be observed by Accredited Audit Service Providers and NIA Certification Service Applicant / NIA Certification subject (auditee) in relation to NIA audit(s) objectives and scopes.

This Technical Directive shall be read in conjunction with the NISCF Audit Standard (NCSA-NISCF-AUD-STND) and NIA Audit Accreditation Standard (NCSA-NISCF-ACCR-AUD-NIA-STND).

2.2. Scope

This Technical Directive applies to all National Information Assurance (NIA) Certification audits.

2.3. About Technical Directives

Technical Directives are documents developed to provide detailed technical requirements about a specific aspect. Unlike Standards and Standard Operating Procedures (SOP), Technical Directives are designed to address a specific topic from all the stakeholders' perspectives (not just from the Accredited Service Provider for NIA Audit).

Technical Directives shall be read and understood by all stakeholders involved in the NIA Certification and shall be viewed as an extension and integrated part of the different policies, standards, processes and procedures documents related to the NISCF's NIA Certification Service and the associated NIA Audit Accreditation Service.

Technical Directives are designed for areas of the NIA Certification Service that have been identified as technically challenging for the Accredited Service Provider for NIA Audit and / or NIA Certification Service Applicant / NIA Certification subject (auditee).

Due to their technical nature and their main objective to overcome challenges faced in processed NIA Certification Service requests by NCSA, Technical Directives are more susceptible to change than Standards and Standard Operating Procedures and on more frequent basis. However, these changes would need to be introduced if it is noted that the original challenges that the Technical Directive was designed to address are not being overcome or when new challenges emerge.

3. Terms and 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-CERT-GTXD (General Taxonomy Document for National Certification - Public), NCSA-NISCF-ACCR-NIA-AUD-STND (NIA Audit Accreditation Standard) and the NCSA-NISCF-AUD-STND (NISCF Audit Standard - Public).

For the purpose of this document, the following verbs indicate:

Appropriate	Suitable for or to.
Can	A modal verb that entail a possibility or capacity.
May	A modal verb that entail a permission.
Shall	A model verb that entail a requirement.
Should	A modal verb that entail a recommendation.

4. Technical Directive

4.1. Audit(s) Objectives

4.1.1.1. The primary objective of National Information Assurance (NIA) Certification audit(s) shall be to perform an audit in conformance with the NISCF Audit Standard and other relevant standards and procedures related to NIA Certification, with specific objectives detailed as below:

- Initial NIA Certification: Provide an audit report that shall allow NCSA to take a Certification decision, on whether to grant or not, a NIA Certificate of Compliance to the applicant;
- Maintenance: Provide an audit report that shall allow NCSA to take a Certification decision, on whether to maintain or not, a NIA Certificate of Compliance of a Certified Organization;
- Re-Certification: Provide an audit report that shall allow NCSA to take a Certification decision, on whether to renew or not, a NIA Certificate of Compliance of a Certified Organization; and
- Special Audits: Provide an audit report that shall allow NCSA to take a Certification decision regarding the objective that will be set by NCSA for the special audit. The objectives of special audits are in most cases either:

  i. Reinstatement After Suspension: Provide an audit report that shall allow NCSA to take a Certification decision, on whether to reinstate or not, a suspended NIA Certificate of Compliance of a Certified Organization; or

  ii. Scope Expansion: Provide an audit report that shall allow NCSA to take a Certification decision, on whether to expand or not, the scope of a NIA Certificate of Compliance of a Certified Organization.

4.2. Scope

4.2.1.1. The scope of audit for NIA Certification shall be the scope of the certification that has been approved by NCSA:

- Initial NIA Certification: The scope of audit shall be the scope approved by NCSA as part of the NIA Certification Service Request;
- Maintenance: The scope of audit shall be either:
  i. The scope of the NIA Certificate of Compliance; or
  ii. The scope expansion part in addition to the scope of the NIA Certificate of Compliance, when NCSA decides that the scope expansion audit shall be performed as part of maintenance.
- Re-Certification: The scope of audit shall be either:
  i. The scope of the NIA Certificate of Compliance; or
  ii. The scope of the NIA Certificate of Compliance and the scope expansion part when the scope expansion request audit has been decided to be performed as part of Re-Certification by NCSA.
- Special Audits: The scope of audit in special audits shall be based on the objective set by NCSA and is generally either:
  i. The scope expansion for scope expansion request audit has been decided to be performed as part of an isolated special audit by NCSA; or
  ii. The scope of a suspended NIA Certificate of Compliance for special audit with the objective of reinstatement following suspension.

4.2.1.2. NIA Certification scope shall be defined by its physical, organizational and logical boundaries (Please refer to NIA Certification Scoping Standard). Therefore:

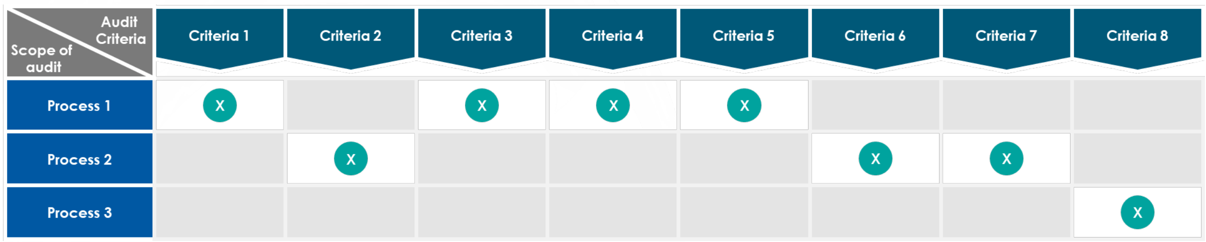
- When the same set of controls (Statement of Applicability), to protect the same business processes, are applied to a location secondary that is different from the NIA Certification primary locations mentioned in the Scope, the secondary location shall not be considered as part of the same scope as this location was not initially mentioned in the scope (subject of the NIA Certification request or the NIA Certificate of Compliance); and

- The list of controls mentioned in the Statement of Applicability (SoA) shall not be considered as the Certification Scope.

4.2.1.3. The scope to be audited is different from the scope of audit. While the scope of audit details the whole NIA Certification scope for each audit type part of the NIA Certification lifecycle, the scope to be audited shall cover which area of the scope of audit (i.e., Certification scope) will be audited during a particular audit to check conformity against specific audit criteria.

4.2.1.4. The Accredited Service Provider for NIA Audit selected shall not audit the entirety of the scope (e.g., processes, departments, locations or products / services) for all the audit criteria as it will be impractical and economically not viable.

The below **Figure 1: Scope to Be Audited Example** is an example a hypothetical scope to be audited (marked with the cross) for a scope of audit including 3 business processes and having 8 audit criteria.



Audit Criteria / Scope of audit	Criteria 1	Criteria 2	Criteria 3	Criteria 4	Criteria 5	Criteria 6	Criteria 7	Criteria 8
Process 1	X		X	X	X			
Process 2		X				X	X	
Process 3								X

Figure 1: Scope to Be Audited Example

4.2.1.5. The Accredited Service Provider for NIA Audit shall develop an Audit Work Program for the full NIA Certification lifecycle (please refer to A.P.2.2.2. Audit Work Program of the NISCF Audit Standard) that allows to cover the entire scope of audit for each audit performed. The Accredited Service Provider for NIA Audit shall instore rotation in the scope to be audited between audits (i.e., shall change the processes that have been audited for a specific NIA Standard domain between audits. This means that if a business process has been audited for Change Management [CM] domain for example, during the initial audit, it shall not be audited for the Change Management [CM] domain, during maintenance and instead, shall be audited for a NIA Standard domain, for which the process was not audited on, in the previous audit).

For more information, please refer to the Standard Operating Procedures on Audit Work Program (NCSA-NISCF-ACCR-AUD-NIA-SOP-AWP) and on Sampling (NCSA-NISCF-ACCR-AUD-NIA-SOP-SAMP).

5. Compliance and Enforcement

5.1. Compliance Process

All applicants to NISCF's NIA Audit Accreditation Services, Accredited Service Provider for NIA Audit, NIA Certification Service Applicants / NIA Certification subject (auditee) by NCSA shall conform with the rules defined in this Technical Directive.

5.2. Roles and Responsibilities

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

5.3. Transitioning and effective date

5.3.1. *Effective date*

This Technical Directive is effective from January 1, 2025.

5.3.2. *Transition period*

New NISCF Certification requests shall conform with this Technical Directive starting from January 1, 2025.

For NISCF Certification requests submitted before January 1, 2025, audits will be conducted as per the NISCF Audit Standard V1.1.

Maintenance, Re-Certification audits and any other audit related to issued NISCF Certificate of Compliance, occurring after January 1, 2025 shall be performed in compliance with this Technical Directive.

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

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

5.4. Exceptions and deviations

5.4.1. *Exceptions to Policy Statements*

Exceptions to this Technical Directive shall only be defined by the National Cyber Security Agency (NCSA) 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 Technical Directive rules shall be formally authorized in writing 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 NIA Audit Accreditation Services and Accredited Service Provider for NIA Audit that do not conform with the requirements defined in this Technical Directive.

National Cyber Security Agency (NCSA) reserves also the right to not accept NIA Certification Service requests and / or suspend or withdraw Certificates of Compliance from applicants to NIA Certification Service Applicants and NIA Certified Organizations that do not conform with the requirements defined in this Technical Directive.

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

NCGAA	National Cyber Governance and Assurance Affairs
NCSA	National Cyber Security Agency
NIA	National Information Assurance
NISCF	National Information Security Compliance Framework
SoA	Statement of Applicability

6.2. 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-ACCR-AUD-NIA-STND (NIA Audit Accreditation Standard - Public)

End of Document