الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

# National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) – Use of the Work of Others

## [NCSA-NISCF-NIA-TD-UWO-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-UWO-001 |
| **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 Technical Directive, titled "National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) – Use of the Work of Others – 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 the use of the work of others during NIA audit, 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) – Use of the Work of Others".

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.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

# 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

**1. Introduction ..... 6**
**2. Purpose and Scope ..... 7**
2.1. Purpose ..... 7
2.2. Scope ..... 7
2.3. About Technical Directives ..... 7
**3. Terms and Definitions ..... 8**
**4. Technical Directive ..... 9**
4.1. The Use of Work of Others ..... 9
4.2. The Use of Previous NIA Certification Work ..... 11
**5. Compliance and Enforcement ..... 12**
5.1. Compliance Process ..... 12
5.2. Roles and Responsibilities ..... 12
5.3. Transitioning and effective date ..... 12
5.4. Exceptions and deviations ..... 12
**6. Annexes ..... 14**
6.1. Acronyms ..... 14
6.2. Reference ..... 15

# 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 the use of the work of others.

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. The Use of Work of Others

### *4.1.1. Work of Others Available for Leverage*

4.1.1.1. The Accredited Service Provider for NIA Audit shall ensure it conforms with the requirements of the A.P.2.2.4. of the NISCF Audit Standard (NCSA-NISCF-AUD-STND) when using the work performed by others.

4.1.1.2. For NIA Certification, the Accredited Service Provider for NIA Audit shall leverage the work performed by others in relation to the scope of the audit when available.

4.1.1.3. In determining the use of the work of others during a NIA audit, the Accredited Service Provider for NIA Audit shall consult with the NIA Certification Subject (Auditee) to determine which works of others can be used to reduce the NIA audit burden.

4.1.1.4. The Accredited Service Provider for NIA Audit shall agree with the NIA Certification Subject (Auditee) on which other audit works will be leveraged during the NIA Certification audit.

The below is a non-exhaustive list of commonly used work of others related to NIA Certification:

- Qatar Cyber Security Framework (QCSF) assessment results performed by NCSA;
- International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27001 Certification and other supporting ISO / IEC 27k family Certifications;
- System and Organization Controls (SOC) 2 Type II report; and
- Payment Card Industry Data Security Standard (PCI DSS) Certification.

### *4.1.2. Use of the Work of Others Considerations*

4.1.2.1.1. When leveraging the work of others, the Accredited Service Provider for NIA Audit shall ensure that the audit criteria covered by the work of others are covering all the audit criteria for the NIA Certification audit.

4.1.2.1.2. The Accredited Service Provider for NIA Audit shall use the mapping provided by the standard owner, or when such mapping does not exist, use reputable source of mapping or develop and justify its own mapping.

4.1.2.1.3. The Accredited Service Provider for NIA Audit shall ensure that the scope of NIA audit is fully covered by work of others.

4.1.2.1.4. The Accredited Service Provider for NIA Audit shall ensure that the conclusions / reports provided by others are still valid. The validity shall be checked within the report itself or attestation (e.g., SOC 2 Type II attestation and its related bridge letter(s)...) or via the Certificate (e.g., ISO / IEC 27001…).

4.1.2.1.5. The Accredited Service Provider for NIA Audit shall ensure that the audit period of the work of others is covering the audit period for the NIA Certification audit.

4.1.2.1.6. The NIA Certification Subject (Auditee) shall provide the mapping between the audit criteria for NIA Certification and the work of others.

4.1.2.1.7. When issues, errors, exceptions or Non-Conformities (NC) reported in the work of others have been resolved before the NIA Certification audit, the NIA Certification Subject (Auditee) shall provide evidence of such resolution and the Accredited Service Provider for NIA Audit shall audit its effectiveness before changing the conclusions provided in the work of others.

4.1.2.1.8. In certain situation, the scope of the work of others is larger than the NIA audit (Certification) scope. When issues, errors, exceptions or Non-Conformities (NC) have been identified in the work of others, but these issues, errors, exceptions or Non-Conformities (NC) are not identified or related to the NIA audit (Certification) scope, the Accredited Service Provider for NIA Audit shall not consider these issues, errors, exceptions or Non-Conformities (NC) as they have not been identified or related to the NIA audit (Certification) scope.

4.1.2.1.9. The Accredited Service Provider for NIA Audit shall adjust the conclusions for the audit criteria based only on the issues, errors, exceptions or Non-Conformities (NC) that have been identified or related to the NIA audit (Certification) scope within the work of others.

4.1.2.1.10. The Accredited Service Provider for NIA Audit shall not ascertain the sample sizes selected in the work of others and shall based on the alignment in terms

of sampling best practices among audit standards and practices that the samples selected in the work of others are representative of the population.

## 4.2. The Use of Previous NIA Certification Work

4.2.1.1.1. The Accredited Service Provider for NIA Audit can be engaged to perform multiple NIA Certification audit(s) on similar scopes in different sites for different NIA Certification requests, or to perform scope expansion audit(s) within a short timeframe from the initial NIA Certification audit. In such situations, the The Accredited Service Provider for NIA Audit can leverage the work performed in previous NIA audit(s), by the Accredited Service Provider for NIA Audit or the previous Accredited Service Provider for NIA Audit. However, this shall only be performed for Design Effectiveness (DE) conclusions only and after ensuring that no changes occurred at the Design Effectiveness (DE) level and that the processes and procedures are applied across the different scope consistently.

# 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