الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) – Corrective Actions Plan

[NCSA-NISCF-NIA-TD-CAP-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-CAP-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) – Corrective Actions Plan – 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 Corrective Actions Plan (CAP), 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) – Corrective Actions Plan".

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

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 Corrective Actions Plan (CAP).

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. Initial Certification Audit Corrective Actions Plan

4.1.1. Pre-Corrective Actions Plan

4.1.1.1. Errors and Findings Confirmation

4.1.1.1.1. As specified in requirement A.P.3.2.2.1 of the NISCF Audit Standard (NCSA-NISCF-AUD-STND), the Accredited Service Provider for NIA Audit shall confirm all the exceptions and errors by discussing with the processes and controls owners to make sure that findings are understood and supported by accurate evidence.

Once exceptions and errors are confirmed, the Accredited Service Provider for NIA Audit should be in a position to build audit conclusions for each audit criterion in the audit on both audit conclusion levels (i.e., Design Effectiveness (DE) and Operating Effectiveness (OE)).

4.1.1.2. Conclusions Building

4.1.1.2.1. The Accredited Service Provider for NIA Audit shall build Design Effectiveness (DE) conclusions based on the professional judgment and professional consensus.

4.1.1.2.2. The Accredited Service Provider for NIA Audit shall build Operating Effectiveness (OE) conclusions based on the tolerable error rate defined at 10%. This means that for any Operating Effectiveness (OE) of an audit criterion for which the extrapolated error rate equals or exceeds 10% the Operating Effectiveness (OE), the conclusion shall be Non-Conformity (NC).

For more information please refer to the audit conclusions classification detailed in section A.P.3.1.6. Findings and Conclusions of the NISCF Audit Standard (NCSA-NISCF-AUD-STND) and the required definition of the associated terminologies.

4.1.1.3. Draft Report

4.1.1.3.1. Once the conclusions are determined and supported by detailed findings and the Accredited Service Provider for NIA Audit confirmed that appropriate and sufficient evidence have been collected, the Accredited Service Provider for NIA Audit shall prepare a draft audit report to be presented during the completion meeting (please refer to requirement

A.P.4.3.1.1 of the NISCF Audit Standard (NCSA-NISCF-AUD-STND) for the deadline to share the draft audit report).

4.1.1.3.2. This draft audit report shall be the basis for the NIA Certification Subject (Auditee) to develop and provide the Corrective Actions Plan (CAP) to address the reported Non-Conformities (NC). When multiple scopes are being audited in the same engagement (e.g., Maintenance of a Certified Scope which includes also the audit of a Scope Expansion request), the common and unique draft audit report provided shall have separate sections for detailed findings and conclusions for each scope.

4.1.1.3.3. As the findings and conclusions have been discussed and agreed with the processes and controls owner prior to drafting the audit report (please refer to section **4.1.1.1. Errors and Findings Confirmation**), following the completion meeting, it is not expected to encounter major updates to the audit report draft that would require the NIA Certification Subject (Auditee) to update the Corrective Actions Plan (CAP) based on the draft audit report. Nevertheless, if such major changes to the draft audit report are required, the Accredited Service Provider for NIA Audit shall provide an updated draft of the audit report without undue delay that enables the NIA Certification Subject (Auditee) to communicate the Corrective Actions Plan (CAP) in conformance with the timeline defined in section **4.1.1.5. Completion meeting**.

4.1.1.4. Completion meeting

4.1.1.4.1. During the completion meeting, the Accredited Service Provider for NIA Audit shall as per requirement A.P.4.2.1.1 of the NISCF Audit Standard (NCSA-NISCF-AUD-STND) present and validate all the findings.

4.1.1.4.2. The NIA Certification Subject (Auditee) shall communicate, to NCSA and the Accredited Service Provider for NIA Audit, the timeline by which it will provide the Corrective Actions Plan (CAP) that shall not exceed ten (10) working days[1] from the completion meeting date.

4.1.2. Corrective Actions Plan

4.1.2.1.1. For all the Non-Conformities (NC), if any, presented in the draft audit report, the NIA Certification Subject (Auditee) shall provide a Corrective Actions Plan (CAP) as per the agreed-on timeframe during the completion meeting.

[1] Excluding National Holidays as declared by Emiri Diwan

The NIA Certification Subject (Auditee) is not required to submit detailed actions and project plan.

4.1.2.1.2. The elements that shall be included in the Corrective Actions Plan (CAP) are:

- Root causes identification of the Non-Conformities (NC);
- General statements regarding the actions that will be taken;
- The verifiable results to be obtained after the implementation of the corrective actions (i.e., the output of the corrective actions); and
- Implementation timeline that shall not exceed six (6) months from the completion meeting date (in determining the timeline of implementation, the NIA Certification Subject (Auditee) should take into consideration the possibility of a follow-up activities during the initial Certification audit and the limited window of time allowed to perform such activities, please refer to section **4.1.4. Follow-up activities during the initial Certification audit** for more information).

4.1.2.1.3. The corrective actions shall encompass actions related to the corrections to be made.

Below is an example providing difference between corrections and root-cause corrective actions. During the audit a Non-Conformity (NC) has been reported for NIA control (audit criteria) AM 4 "A process is established which, upon any employee role or status change (including termination) ensures that information system access is updated to reflect the employee's new role", at the Operating Effectiveness (OE) level. Indeed, there was three (3) accounts of two (2) employees that had been identified as active while these employees left the NIA Certification Subject (Auditee) organization. The root-cause has been identified by the NIA Certification Subject (Auditee) that the Human Resources (HR) department is not communicating on time and systematically employees' terminations. The Corrective Actions Plan (CAP) shall include for example:

- Corrective actions to address the root-cause: Update the process to include the Information Technology and Systems department in the group of departments notified by any change of role including terminations; and
- Corrections: Deactivate the three (3) accounts.

The NIA Certification Subject (Auditee) may include more details in the Corrective Actions Plan (CAP) such as dependencies, key success factors, required resources, project(s) owner(s)…

4.1.2.1.4. The NIA Certification Subject (Auditee) shall include in the Corrective Actions Plan (CAP), if it is not practically or chronologically feasible to implement corrections, activities to build preventive controls that aims at avoiding re-occurrence of the Non-Conformities (NC).

4.1.3. Corrective Actions Plan assessment and reporting

4.1.3.1.1. The Accredited Service Provider for NIA Audit shall assess Corrective Actions Plan (CAP) to evaluate if the actions are appropriate and address the root-causes of the Non-Conformities (NC).

4.1.3.1.2. The results of this assessment shall be included in the final version of the audit report as mentioned in requirement A.P.4.3.1.4 of the NISCF Audit Standard (NCSA-NISCF-AUD-STND).

4.1.3.1.3. The final version of the audit report shall also mention for each Non-Conformity (NC) the date and the person that performed the acknowledgment of the Non-Conformity (NC) from NIA Certification Subject (Auditee).

4.1.3.1.4. The Accredited Service Provider for NIA Audit shall provide the applicant to NIA Certification Service, the NIA Certification Subject (Auditee) and NCSA the final version of the audit report within ten (10) working days[2] from the communication of the Corrective Actions Plan (CAP) by the NIA Certification Subject (Auditee).

4.1.4. Follow-up activities during the initial Certification audit

As defined in the NIA Certification Processes document (NCSA-NISCF-CERT-NIA-POSS) under the section 4.2.1 NIA Certification Process – Step 11, NCSA can decide to request additional audit work from the Accredited Service Provider for NIA Audit before taking the final decision of granting or denying the NIA Certification.

This additional audit work may consist in auditing the effectiveness; in Design Effectiveness (DE) and Operating Effectiveness (OE) depending of the audit conclusions levels related to the Non-Conformities (NC); of the Corrective Actions Plan (CAP). NCSA will consider the proposed

[2] Excluding National Holidays as declared by Emiri Diwan

implementation timeline for the Corrective Actions Plan (CAP) prior of taking the decision to request follow-up activities during the initial Certification audit.

The follow-up activities should be conducted and completed by the Accredited Service Provider for NIA Audit as soon as possible, ideally in a period that does not exceed fifteen (15) working days[3] from the date of NCSA's request for additional audit work.

4.1.4.1.1. The Accredited Service Provider for NIA Audit shall provide an updated audit report based on the additional audit work, reporting the updated audit conclusions based on the audit of the effectiveness of the implementation of the Corrective Actions Plan (CAP) and with audit findings explaining the conformity to audit criteria before and after the additional audit work performed (in order to provide a full and complete view of the conformity status during the entirety of the initial Certification audit).

4.2. Subsequent audit(s)

4.2.1. Follow-up on Non-Conformities (NC) reported during previous audit(s)

4.2.1.1.1. When Corrective Actions Plan (CAP) for identified Non-Conformities (NC) has been developed following the completion of an audit and no follow-up activities where performed, the audit of the effectiveness of the implementation of the Corrective Actions Plan (CAP) shall be performed the during the subsequent audit (i.e., Maintenance, special audit for reinstatement after suspension, Re-Certification).

Certain of these audit(s) are mainly focused on this aspect (i.e., Maintenance, special audit for reinstatement after suspension), while in the Re-Certification the effectiveness of the implementation of the Corrective Actions Plan (CAP) is generally a relatively small part of the audit.

4.2.2. Corrective Actions Plan based on subsequent audit(s)

4.2.2.1.1. The basis, preparation, communication, assessment and reporting related to Corrective Actions Plan (CAP) related to Maintenance, special audit(s) and Re-Certification shall follow the same rules as the initial Certification audit Corrective Actions Plan (CAP) defined in section **4.1. Initial Certification Audit Corrective Actions Plan**.

[3] Excluding National Holidays as declared by Emiri Diwan

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