الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

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

[NCSA-NISCF-NIA-TD-AC-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-AC-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) – Audit Calendar – 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 calendar, 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 Calendar".

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

Table of Tables

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 calendar.

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 Calendar Conformity Pre-requisites

4.1.1.1.1. The Accredited Service Provider for NIA Audit shall ensure documents, information and person(s) are available as per the plan to conform with the mentioned timeline in this Technical Directive and the requirements of the NISCF Audit Standard (NCSA-NISCF-AUD-STND) and the NISCF Standard for Management Systems' Certification (NCSA-NISCF-CERT-SMSC).

4.1.1.1.2. The Accredited Service Provider for NIA Audit shall report to NCSA, without undue delays, if there is an indicator that these timelines will not be observed and provide clear reasons that led to this delay and the corrective actions to address the delay.

4.1.1.1.3. The Accredited Service Provider for NIA Audit shall deploy the adequate and sufficient resources (technical and human) to complete the audit(s) as per the different timeline set in this Technical Directive and the requirements of the NISCF Audit Standard (NCSA-NISCF-AUD-STND) and the NISCF Standard for Management Systems' Certification (NCSA-NISCF-CERT-SMSC) and therefore shall adequately size the audit team considering these timelines.

The Accredited Service Provider for NIA Audit should also allow for a buffer to accommodate for any unexcepted situations allowing to manage these situations without exceeding the determined timelines.

4.1.1.1.4. The NIA Certification subject (auditee) shall prepare for the audit accordingly, agree with the Accredited Service Provider for NIA Audit and commit on an audit calendar that shall conform with the mentioned timeline in this Technical Directive and the requirements of the NISCF Audit Standard (NCSA-NISCF-AUD-STND) and the NISCF Standard for Management Systems' Certification (NCSA-NISCF-CERT-SMSC).

The NIA Certification subject (auditee) should, prepare in advance evidence repository and ensure it has readily available the expected documentation and evidence related to the Information Security Management System.

4.1.1.1.5. The NIA Certification subject (auditee) shall make available the key resources for NIA Certification audit and respond in the defined delays to Accredited Service Provider for NIA Audit and NCSA requests.

4.2. Initial NIA Certification Application and Audit Calendar

4.2.1.1. The overall audit calendar length and the timeline needed to perform each activity for the initial NIA Certification audit shall be based on justification and factors' assessment (please refer to **Figure 3: Design Effectiveness (DE) Audit Calendar Scale Factors** and **Figure 4: Operating Effectiveness (OE) Audit Calendar Scale Factors**).

4.2.1.2. The below table details the audit calendar main activities and the maximum allowed timeline to completed them. The below presents the maximum allowed period for each activity and shall not be taken as the "default" timeline to perform the activities.

Domain	Activity ID	Description	Owner	Start	Maximum allowed timeline	Period Type	Reference
Request	RQST-1	Submitting NIA Certification Service Request	NIA Certification Applicant	-	-	-	4.2.1.1. NISCF Standard for Management Systems' Certification
Request	RQST-2	Scope approval (and invoicing application fees) or rejection, including intermediate Clarification and Evidence Requests (CER), if any	NCSA	RQST-1	60	Calendar days	4.2.1.2.3. NISCF Standard for Management Systems' Certification
Request	RQST-3	NIA Application fees payment	NIA Certification Applicant	RQST-2	30	Calendar days	11.2. NIA Certification Terms and conditions

Domain	Activity ID	Description	Owner	Start	Maximum allowed timeline	Period Type	Reference
Initial Audit	IAUD-1	Choose an Accredited Service Provider for NIA Audit and informing it about the selection	NIA Certification Applicant	RQST-2	60 (suggested not mandatory)	Calendar days	This Technical Directive
Initial Audit	IAUD-2	Complete acceptance due diligence	Accredited Service Provider for NIA Audit	IAUD-1	15 (suggested not mandatory)	Calendar days	This Technical Directive
Initial Audit	IAUD-3-A	Signature of the Engagement Letter	NIA Certification Applicant / Accredited Service Provider for NIA Audit	IAUD-2	15 (suggested not mandatory)	Calendar days	This Technical Directive
Initial Audit	IAUD-3-B	Signature of the Engagement Letter	NIA Certification Applicant / Accredited Service Provider for NIA Audit	RQST-2	180	Calendar days	4.2.2.2.2. NISCF Standard for Management Systems' Certification
Initial Audit	IAUD-4	Preliminary Work and Planning	Accredited Service Provider for NIA Audit	IAUD-3	10	Working days	This Technical Directive
Initial Audit	IAUD-5	Perform and Complete Design Effectiveness (DE) audit	Accredited Service Provider for NIA Audit	IAUD-4	10	Working days	This Technical Directive
Initial Audit	IAUD-6	Design Effectiveness (DE) Reporting (intermediate) to NCSA	Accredited Service Provider for NIA Audit	IAUD-5	5	Working days	A.P.4.1.1.2. NISCF Audit Standard
Initial Audit	IAUD-7	Implement Design Effectiveness (DE) Non-Conformities (NC) corrections, if any	NIA Certification Subject (Auditee)	IAUD-6	30	Calendar days	This Technical Directive

Domain	Activity ID	Description	Owner	Start	Maximum allowed timeline	Period Type	Reference
Initial Audit	IAUD-8	Perform and complete Operating Effectiveness (OE) audit and Design Effectiveness (DE) update, share draft audit report to NCSA and organize and hold a completion meeting	Accredited Service Provider for NIA Audit	IAUD-6 / IAUD-7	20	Working days	This Technical Directive
Initial Audit	IAUD-9	Corrective Actions Plan (CAP), if any	NIA Certification Subject (Auditee)	IAUD-6	10	Working days	4.1.1.4.2. Technical Directive on Corrective Actions Plan
Initial Audit	IAUD-10-A	Submit final audit report to NCSA	Accredited Service Provider for NIA Audit	IAUD-8 / IAUD-9	10	Working days	4.1.3.1.4. Technical Directive on Corrective Actions Plan / A.P.4.3.1.2. NISCF Standard for Management Systems' Certification
Initial Audit	IAUD-10-B	Submit final audit report to NCSA	Accredited Service Provider for NIA Audit	RQST-1	365	Calendar days	4.2.1.2.6. NISCF Standard for

Domain	Activity ID	Description	Owner	Start	Maximum allowed timeline	Period Type	Reference
							Management Systems' Certification
Closing / Award	CLAW-1	Audit Review, Clarification and Evidence Requests (CER), if any and Certification decision (and invoicing Certification fees if granted)	NCSA	IAUD-10	30 (suggested not mandatory)	Calendar days	This Technical Directive
Closing / Award	CLAW-2	Perform follow-up activities, if requested by NCSA	Accredited Service Provider for NIA Audit	CLAW-1	15 (suggested not mandatory)	Working days	Section 4.1.4 Technical Directive on Corrective Actions Plan
Closing / Award	CLAW-3	Certification decision (and invoicing Certification fees if granted), if follow-up activities are performed	NCSA	CLAW-2	30 (suggested not mandatory)	Calendar days	This Technical Directive
Closing / Award	CLAW-4	Application fees payment	NIA Certification Applicant	CLAW-1 / CLAW-3	30	Calendar days	11.2. NIA Certification Terms and conditions

Table 1: Calendar for NIA Certification Application, Audit and Closing

Please refer to the **Figure 1: Initial Certification Audit Calendar** for illustrative graphical representation of the initial NIA Certification audit calendar and main deadlines.

4.3. Other Audit(s) Calendar

4.3.1. Maintenance

4.3.1.1. Maintenance shall be completed within one (1) month from its start.

Maintenance audit budget should represent [15% - 30%] of the initial NIA Certification audit budget. This depends on the number of Non-Conformities (NC) to be audited based on the Corrective Actions Plan (CAP) and the changes occurred in the scope subsequent to the latest audit that would require re-auditing.

4.3.2. Re-Certification

4.3.2.1. Re-Certification shall be completed before the expiry date of the NIA Certificate of Compliance.

Re-Certification audit budget should represent [50% - 65%] if there are no changes to the scope subsequent to the latest audit that would require re-auditing.

Please refer to the **Figure 2: Re-Certification Audit Calendar** for illustrative graphical representation of the Re-Certification audit calendar and main deadlines.

4.3.3. Scope Expansion

4.3.3.1. The Accredited Service Provider for NIA Audit shall use the Design Effectiveness (DE) and Operating Effectiveness (OE) audit calendar factors (please refer to **Figure 3: Design Effectiveness (DE) Audit Calendar Scale Factors** and **Figure 4: Operating Effectiveness (OE) Audit Calendar Scale Factors**) to determine the audit calendar for an audit of scope expansion.

4.4. Time Distribution

4.4.1.1. The Accredited Service Provider for NIA Audit shall divide the available audit budget and calendar across the different audit phases in a manner that will allow the completion of the audit in the defined timelines.

The below table is a guidance on the audit budget and calendar distribution across the three (3) main audit phases.

Phases	Budget consumption	Spread During Audit	Description
Planning	20%	Long	Planning is performed from the start of the audit and go all the way until the reporting is completed. Therefore, even though it generally consumes about 20% of the time budget, planning activities tend to spread across a long period in the audit calendar.
Execution and Supervision	60%	Short	Performing field audit activities is the phase that would require from the Accredited Service Provider for NIA Audit and NIA Certification Subject (Auditee) the most effort and time budget. However, in order to limit the effect of the disruption of the audit on the NIA Certification Subject (Auditee) operation, the execution phase should be performed in the shortest timeline possible. Audit execution should be condensed in a short period in the audit calendar allowing for resources (from both sides) to dedicate to the audit for a short period of time and allowing the NIA Certification audit to be completed in a manageable timeline.
Reporting and completion	20%	Average	Reporting starts once Design Effectiveness (DE) audit is completed and continues until the end of the audit. During reporting, the audit team has a clear understanding and view of the scope and should be able to perform the reporting activities in relatively quicker manner than planning for example. However, due to the fact that there are multiple reporting to be performed, reporting tend to spread over around half the audit calendar.

Table 2: Time Distribution Guideline

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

CAP	Corrective Actions Plan
CER	Clarification and Evidence Request
DE	Design Effectiveness
NCGAA	National Cyber Governance and Assurance Affairs
NCSA	National Cyber Security Agency
NIA	National Information Assurance
NISCF	National Information Security Compliance Framework
OE	Operating Effectiveness

6.2. Tables, Graphs and Figures

6.2.1. *Initial Certification Audit Calendar Graph*

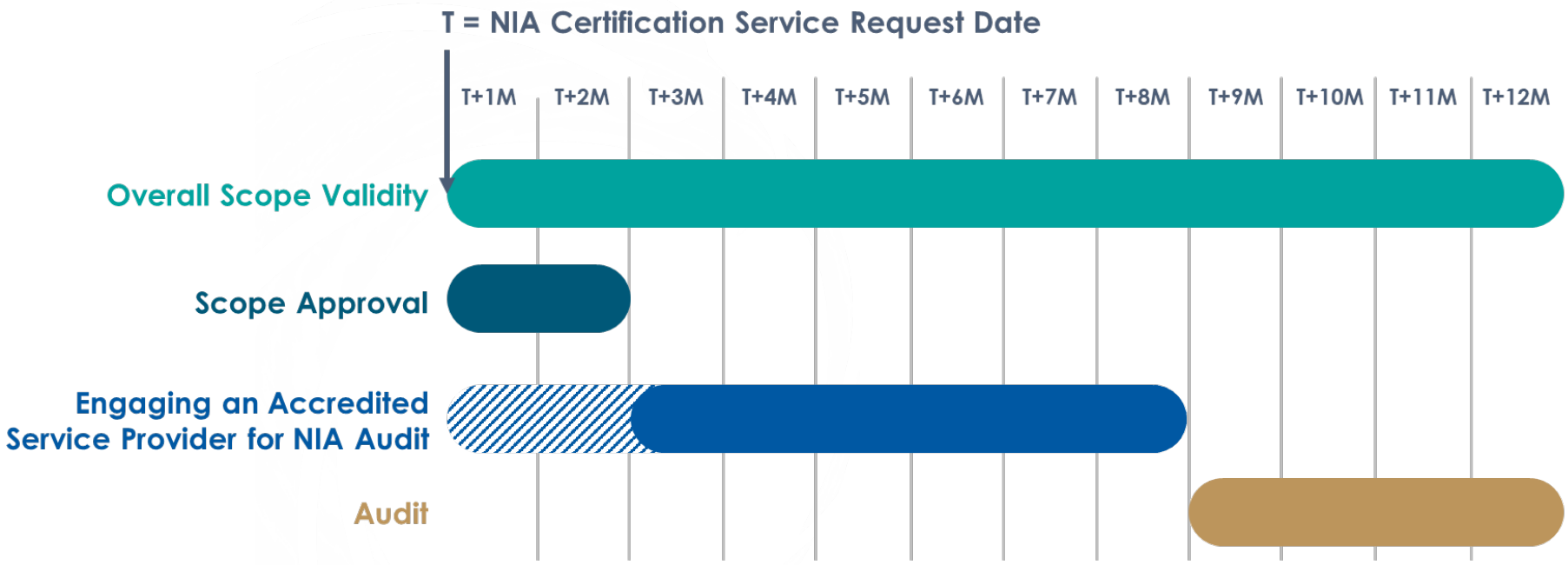

Figure 1: Initial Certification Audit Calendar

6.2.2. *Re-Certification Audit Calendar Graph*

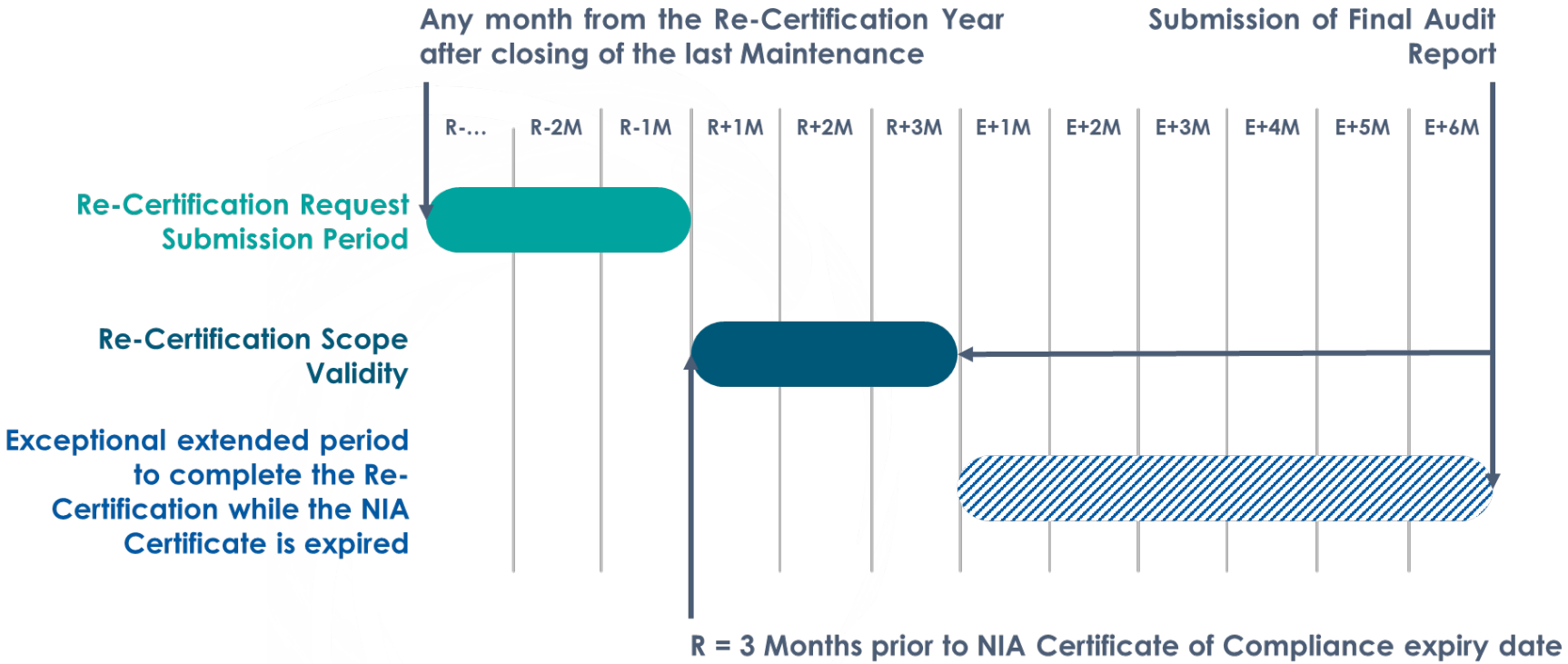

Figure 2: Re-Certification Audit Calendar

6.2.3. Design Effectiveness (DE) Audit Calendar Scale Factors Graph

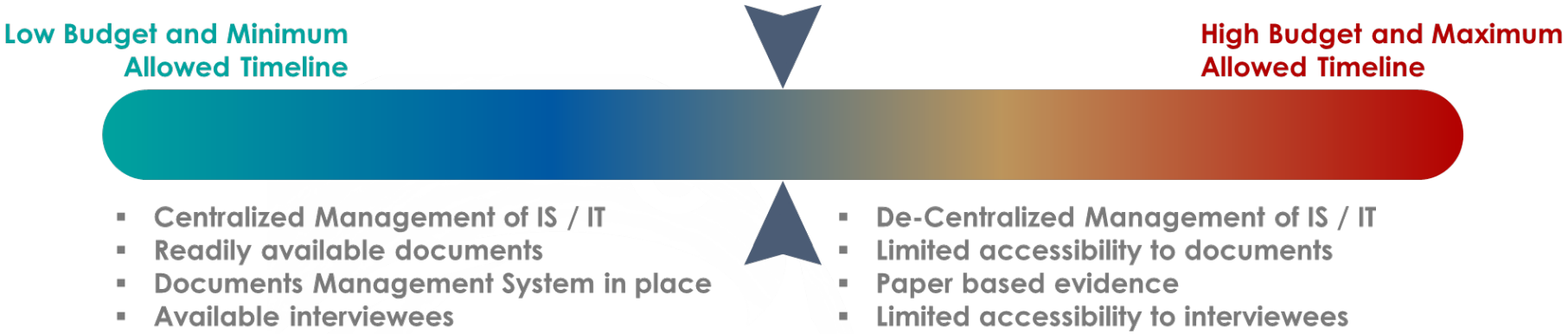

Figure 3: Design Effectiveness (DE) Audit Calendar Scale Factors

Regardless of the complexity and the size of the scope, when using the work of others, the Design Effectiveness (DE) and Operating Effectiveness (OE) audit calendar shall be converging toward the minimum allowed timeline.

6.2.4. *Operating Effectiveness (OE) Audit Calendar Scale Factors Graph*

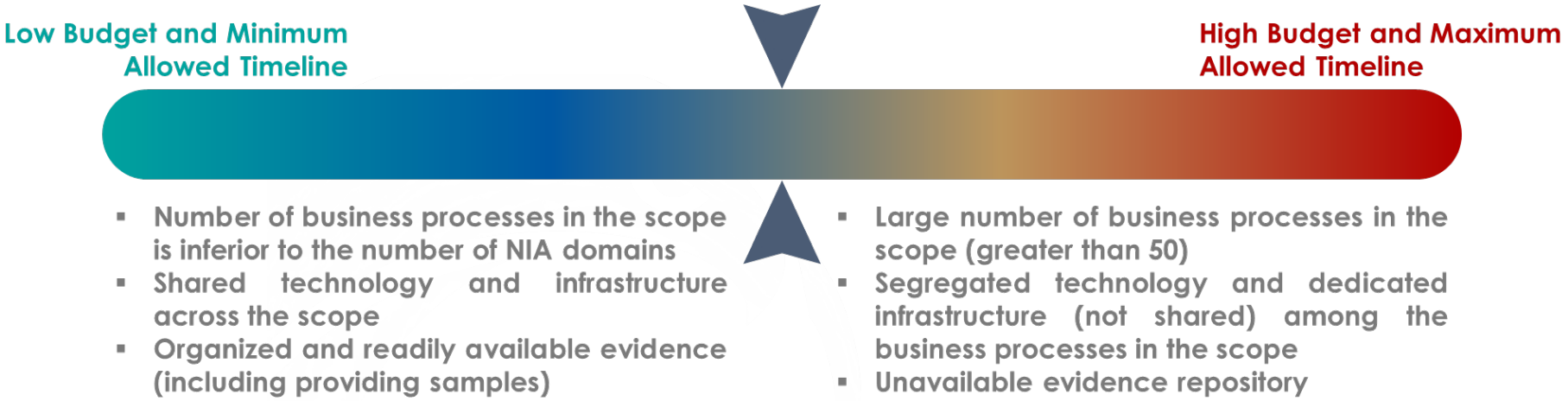

Figure 4: Operating Effectiveness (OE) Audit Calendar Scale Factors

Regardless of the complexity and the size of the scope, when using the work of others, the Design Effectiveness (DE) and Operating Effectiveness (OE) audit calendar shall be converging toward the minimum allowed timeline.

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

End of Document