الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

National Information Security Compliance Framework (NISCF) – Audit Standard

[NCSA-NISCF-AUD-STND]

Audit Requirements

National Cyber Security Agency (NCSA)

October 2024

V3.0

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

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Document Control

Document Details	
Document ID	NCSA-NISCF-AUD-STND
Version	V3.0
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 – Audit Standard" - V3.0 - C0 – Public / PS1 – Non-Personal Data (Non-PD), in order to provide the requirements for applicants to NISCF's Audit Accreditation Services, Accredited Service Providers and for the delivery of Audits related to NISCF's Services, 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 – Audit 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.

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.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

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.

Service Providers shall comply with the requirements defined in this standard and other audit standard specific to NISCF's Services, for the purpose of obtaining Accreditation and ongoing maintenance.

2. Purpose and Scope

2.1. Purpose

The purpose of this document is to provide requirements for organization willing to request for NISCF's Audit Accreditation Services, Accredited Audit Service Providers and for the delivery of audits related to NISCF's Services. This document also helps applicants to NISCF Services, in which audit is required, to understand the audit that they will be subject to.

There is potential Cyber Assurance Services offered by NCSA under the NISCF, that may not require an audit in order to provide the required level of Assurance. These Cyber Assurance Services will rely on Assessments, Reviews, Evaluations and / or Examinations which do not have to conform to standards, processes, procedures and rules that are as rigorous as the ones governing an audit.

Therefore, each requirement defined in this Audit Standard can be used solely or in combination with other requirements, partially or fully, to govern Assessments, Reviews, Evaluations and / or Examinations under NISCF.

NCSA will define through the specific standards, agreements, procedures and terms and conditions related to the Cyber Assurance Services that require Assessments, Reviews, Evaluations and / or Examinations which requirements defined in this Audit Standard are required to be followed in these exercises.

This standard can also be used by regulatory authorities, after approval from NCSA, as audit standard.

2.2. Scope

This document applies to all applicants to NISCF's Audit Accreditation Services, Accredited Audit Service Providers and the audits they deliver related to the NISCF's Services.

NCSA defines which NISCF's Services this document applies to.

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

In case a terminology is defined in this document and is also defined in the above-mentioned documents, the definition provided in this document supersede these ones defined in the other documents.

Acceptance	The phase of the audit in which the Service Provider assess if it can engage with the client and formally document its decision.
Analytical procedure	A type of audit procedure that consists of evaluations of a data set through the study of the plausible relationships and trends and the detection of outliers.
Audit	Process for obtaining appropriate and sufficient evidence about a scope and evaluating it objectively, in conformance with specific evaluation standards, methods and procedures to determine conformance of the scope to defined audit criteria.
Audit assertions	Declarations made by the management about the underlying subject(s) matter and the Scope(s) of audit(s). Assertations can be declarative or results from the adoption of a standard or framework by the management.
Audit criteria	The reference point(s) or benchmark(s) used in a specific audit to measure or evaluate the underlying subject matter conformance.
Audit period	The historical period for which the compliance of the scope and the conformance of underlying subject(s) matter to audit criteria will be verified during the audit.
Audit risk	The risk of reaching an incorrect conclusion based upon audit findings.

Audit testing script	Step-by-step tasks that shall be self-explanatory for an auditor to perform the defined audit procedures and clearly reflecting the nature and timing of the audit procedures and the extent consideration.
Auditor	Person(s) designated by the Service Provider, considered as audit team member, conducting audit activities.
Bias	Systematic inclination toward a person, group or organization that leads to the objectivity of audit team members to be compromised.
Computer-Assisted Audit Tools (CAATs)	Software that are design to facilitate and enhance the audit process. These include mainly audit Software, utility software, plotting and cartography software and audit expert systems.
Conclusion	Outcome of execution of audit procedures on the underlying subject matter for an audit criterion based on a finding.
Confirmation	A type of audit procedure that seeks to obtain a particular form of audit evidence from a third-party (other than the auditee).
Control risk	The risk that a material non-conformity (leading to non-compliance) could occur and will not be prevented, detected or corrected at the right time by auditee's existing controls.
Design Effectiveness (DE)	Level of audit conclusion focusing the adequate design to comply with the audit criteria. This level focuses also on the documentation of the designed controls and its approval as well as the communication to the processing and affected parties.
Detection risk	The risk that the audit procedures that are performed or to be performed by the Service Provider will not detect a material non-conformity.
Endorsement and Advocacy	Defend, promote, provide endorsement to or champion, the organization engaging the Service Provider or the organization(s) subject of the audit, in way that the Service

	Provider or the audit team member will not be able to maintain impartiality and objective judgment.
Engagement Lead	Person designated by the Service Provider, considered as audit team member, that is: • Accountable for all the deliverables of the audit; • Manage stakeholders and ensure the audit objectives are met; and • Serve as escalation point and resolve important challenges that arise.
Extent of audit procedures	The quantity and number of times an audit procedure will be performed.
Fair and faithful representation	A depiction that is: • Neutral: That is not slanted, mis-represent weights and probabilities or asymmetric in terms of risk aversion; • Correct: That does not contain material errors or omissions from the Service Provider in relation to the audit activities performed; and • Complete: That provide a full view of the compliance of the scope to the defined audit criteria, for the defined audit period, and this based on the defined audit activities that comply with the requirements defined in this standard and other relevant NISCF standards specific to the NISCF's Service requiring the audit.
Familiarity	Extended or close relationship between: • The organization engaging the Service Provider or the organization(s) subject of the audit, persons in charge of their governance and / or management and employees; and • The Service Provider, the audit team member or an organization part of its firm network;

	resulting to inappropriate judgment or behavior by the audit team members due to sympathy or family relation.
Finding	Detailed results from applied audit procedure on collected audit evidence for specific underlying subject(s) matter detailing the conformity or not to audit criteria that serve as a basis, individually or in combination with other finding(s) for a conclusion.
Guide	A person designated by the client to assist and help logistically the audit team during the audit.
Independent Quality Control Reviewer (IQCR)	A person designated by the Service Provider to perform the quality control checks defined as per the NISCF requirements.
Information Assets	A body of information, defined and managed as a single unit, so that it can be understood, shared, protected and utilized effectively. Information Assets can be processed in a physical (i.e., paper), digital (i.e., IT / OT) or cognitive (i.e., human knowledge) format.
Inherent risk	The risk level or exposure of the scope susceptibility to a material non-conformity (leading to non-compliance) without considering what actions the auditee has or could take to mitigate those risks.
Inquiry	A type of audit procedure that consists of gathering information from relevant stakeholders, orally or in written.
Inspection	A type of audit procedure that involves examining documents in any format or physically examining an asset.
Intimidation	Undue influence by the organization engaging the Service Provider or the organization(s) subject of the audit, persons in charge of their governance and / or management and employees over the Service Provider, the audit team member or an organization part of its firm network, that will directly or

	indirectly, result in the inability to maintain impartial and objective judgment.
Lead Auditor	Person designated by the Service Provider, considered as audit team member, that is: • Responsible for the audit and its management until its completion; and • Review all the deliverables of the audit.
Material	Important factor that can be reasonably expected to affect a decision.
Nature of audit procedures	The purpose (test of control or substantive procedure) and type of an audit procedure. A type of audit procedure that consists of looking at the underlying subject(s) matter being processed or performed by the operator.
Observer	A person that accompanies the audit team members and does not have any audit task to perform.
Operating Effectiveness (OE)	Level of audit conclusion focusing the effective running as designed. The level focuses on the effective avoidance, detection and treatment of exceptions and errors.
Opportunities For Improvements (OFI)	Areas of apparent possibilities for improving a results-centered process / control for increased efficiency or a better outcome. An OFI is a suggestion and is not a Non-Conformity as it is not based on an audit criterion. OFIs have for objective to prevent the potential occurrence of a Non-Conformity in the future.
Organization being audited	The legal entity to which the scope of the NISCF's Service request being audited is related.

Organization engaging the Service Provider	The legal entity that contractually engages the Service Provider to perform the audit.
Partner	Organization that has contractual relationship with the Service Provider in relation to the audit.
Professional skepticism	A mind set and attitude to be observed by the audit team members that allows individual(s) to have a questioning mind, being alert to material aspects and having critical thinking.
Proficiency	Advanced (applied theory) skills and expertise.
Precomputation/ Reperformance	A type of audit procedure that consists of computing numbers and / or execute transactions, procedures or controls that were performed by the auditee in order to verify the mathematical accuracy of transactions or records and / or output of procedures.
Related parties	Related parties for a specific organization are: • A person or organization that has control or significant influence, directly or indirectly, over the organization engaging the Service Provider and the organization(s) being audited; • An organization over which the organization engaging the Service Provider and / or the organization(s) being audited have control or significant influence, directly or indirectly; or • An organization under the common control with the organization engaging the Service Provider and / or the organization(s) being audited. Government entities are not considered related parties.
Risk of material non-conformities	The residual risk when combining the inherent risk and control risk.

Safeguards	Actions, individually or in combination, that are taking by the Service Provider and / or third-party organizations or individuals, trusted with the responsibility, to mitigate threats of conflict of interests based on the Risk Management System of the Service Provider.
Sampling risk	The risk that the Service Provider's conclusion based on a sample would be different from the conclusion that it would have made if the entire population were tested by to the same audit procedure.
Scope(s) of audit(s)	Specifies the extent and boundaries of the Scope(s) of audit(s).
Scope of work	Description of the work to be performed by the Service Provider in relation to an audit that is defined or reference in a contractual agreement. The scope of work is different from the Scope(s) of audit(s).
Self-Interest	Interest from the Service Provider or the audit team members, financial or other, that will inappropriately influence judgment or behavior.
Self-Review	The Service Provider or the audit team members inappropriately evaluating the outputs of previous judgment made by the Service Provider, an audit team member or an organization part of the firm network of the Service Provider.
Technical Expert	A person that provides specific expertise (other than audit) to the audit team on a specific technical topic or issue.
Timing of audit procedures	When an audit procedure will be performed.
Tolerable NC rate	The maximum number of errors in the population that the Service Provider can accept to be able to still conclude that the audit criteria objective is still achieved.

Underlying subject(s) matter	Elements that constitute the population to be tested by the Service Provider considering the audit assertions, criteria, and period. Underlying subject matter can vary based on the objective of the audit criteria and audit procedure. It can be an information asset, a transaction / event, a location, person, or a system...
Whistleblowing	Activity of a person reporting activity within an organization or a project that is either illegal, illicit, unethical or fraudulent.
Working papers	Audit documentation that records all the details of a specific or a group of audit activities conducted, including: • The objective of the working paper; • who conducted the audit activities and who reviewed it; • Reference or recording of the nature, extent and timing of the audit procedures and the related audit testing script; • The underlying subject(s) matter and samples; • The interviewed individuals and the requested documents and records; • The findings and conclusions related to the audit procedures applied; and • Any other matter that the Service Provider judges to be important to record.

4. Standard Requirements

A.C.E. Audit Control Environment

A.C.E.1. Audit Principles

A.C.E.1.1. Ethical and Professional Conduct

A.C.E.1.1.1.1. The Service Provider and its audit team members shall commit to adhering, complying and conforming at all time to the rules and requirements defined in section **A.C.E.2.3. Code of Ethics and Professional Conduct**.

A.C.E.1.1.1.2. The Service Provider and its audit team members shall act in ethical and professional manner at all time.

A.C.E.1.1.1.3. The Service Provider and its audit team members shall apply the audit principles defined in this section at all time.

A.C.E.1.1.1.4. The Service Provider and its audit team members shall adhere, comply and conform with the requirements defined in this standard when conducting an audit.

A.C.E.1.2. Proficiency

A.C.E.1.2.1.1. The Service Provider shall possess adequate proficiency in auditing encompassing:

- Familiarity with the audit criteria;
- Understanding of the industry within which the audited organization(s) operate;
- Comprehension of the processes, organizational structures, and operational frameworks within the audit scope; and
- Proficiency in the systems and technologies utilized within the audit scope.

A.C.E.1.2.1.2. The audit team members shall possess collectively the proficiency required to complete the audit in conformance with the requirements defined in this standard.

A.C.E.1.3. Evidence-Based Audit

A.C.E.1.3.1.1. The Service Provider shall adhere to an evidence-based audit methodology during audits, ensuring reliable and reproducible conclusions

within the constraints of finite duration and resources, enabling conformance with requirements related to audit risk defined in this standard.

A.C.E.1.4. Risk-Based Audit

A.C.E.1.4.1.1. The Service Provider shall employ a risk-based audit approach to prioritize material aspects during audits.

A.C.E.1.4.1.2. The Service Provider shall adopt this approach in all phases of the audit process, as defined in section **A.P. Audit Process**.

A.C.E.1.5. Reasonable Expectation

A.C.E.1.5.1.1. The Service Provider shall build, throughout the entire audit, reasonable expectation that the audit activities can be conducted in conformance with applicable laws and regulations.

A.C.E.1.5.1.2. The Service Provider shall build, throughout the entire audit, reasonable expectation that the audit activities can be conducted in conformance with this standard and any other relevant NISCF policies, standards, processes, terms and conditions, specific to the NISCF's Service requiring the audit.

A.C.E.1.5.1.3. The Service Provider shall have, before the planning of the audit, reasonable expectation that the organization engaging the Service Provider, and its management understand their obligations and responsibilities in relation to the audit and NISCF's Service requiring the audit.

A.C.E.1.5.1.4. The Service Provider shall identify, and work with the client[1] to address, the potential limitations, including but not limited to:

- Restrictions related to access to relevant, appropriate and timely, information;
- Restrictions related to access infrastructures, locations and systems;
- Unavailability of key individuals;
- Changes occurring or planned to occur during the audit that would, in the Service Provider judgment, affect the scope or the client; and

[1] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

- Insufficient audit timeline.

A.C.E.1.6. Faithfull and Fair Representation

A.C.E.1.6.1.1. The Service Provider shall, in all its audit documentation, record a fair and faithful representation of the:

- Compliance of the scope or a sub-set of the scope to the audit criteria or a sub-set of the audit criteria;
- Audit activities performed or planned to be performed; and
- Statements and information provided by the client[2].

A.C.E.1.6.1.2. The Service Provider shall not use comparative or superlative adjectives in its reporting.

A.C.E.2. Audit Resources Governance

A.C.E.2.1. Key Audit Roles

A.C.E.2.1.1. Audit Team Composition

A.C.E.2.1.1.1. All individuals chosen by the Service Provider to engage in audit activities, as outlined in section **A.P. Audit Process**, irrespective of their contractual status, shall be recognized as members of the audit team.

A.C.E.2.1.1.2. All audit team members shall be contractually bound with the Service Provider, either directly or indirectly through third parties, and authorized to perform the designated audit tasks, taking into consideration requirements **A.C.E.2.1.2.1** and **A.C.E.2.1.3.1**.

A.C.E.2.1.1.3. Observers, interpreters, Technical Experts and Independent Quality Control Reviewer (IQCR) shall not be considered as audit team members and shall not be assigned any audit activity, except for Technical Experts.

A.C.E.2.1.1.4. The Service Provider shall ensure that observers, interpreters, Technical Experts and Independent Quality Control Reviewer (IQCR) act in conformance with the **A.C.E.2.3. Code of Ethics and Professional Conduct**.

A.C.E.2.1.1.5. The Service Provider shall be accountable for observers, interpreters and Technical Experts actions during the audit.

[2] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

A.C.E.2.1.1.6. The Service Provider shall define and agree with the client[3] of the role of Technical Experts, before performing the audit.

A.C.E.2.1.1.7. The Independent Quality Control Reviewer (IQCR) shall review the below, for conformance with this standard and other relevant NISCF standards specific to the NISCF's Service requiring the audit, before communication with NCSA and / or the client:

- Client / Engagement Acceptance and Relationship Continuance evidence;
- Planning documentation; and
- Audit Report.

A.C.E.2.1.1.8. The IQCR shall occupy a similar or higher organizational position in the Service Provider structure than the Engagement Lead.

A.C.E.2.1.1.9. The IQCR shall evidence sufficient audit and cyber security knowledge and experience to perform the required tasks defined in requirement **A.C.E.2.1.1.7**.

A.C.E.2.1.2. Engagement Lead

A.C.E.2.1.2.1. The Service Provider shall ensure that the Engagement Lead is not outsourced.

A.C.E.2.1.2.2. The Service Provider shall appoint a unique Engagement Lead for each audit (please refer to the Engagement Lead definition in section **3. Terms and Definitions**).

A.C.E.2.1.3. Lead Auditor

A.C.E.2.1.3.1. The Service Provider shall ensure that the Lead Auditor is not outsourced.

A.C.E.2.1.3.2. The Service Provider shall appoint a unique Lead Auditor for each audit (please refer to the Lead Auditor definition in section **3. Terms and Definitions**).

A.C.E.2.1.4. Auditor

A.C.E.2.1.4.1. The Auditor shall only conduct audit activities assigned to him / her and under the supervision of the Lead Auditor and / or the Engagement Lead.

[3] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

A.C.E.2.1.4.2. The Auditor shall understand the responsibility he / she has in the context of the audit.

A.C.E.2.1.4.3. The Auditor shall report to the Lead Auditor or the Engagement Lead, any practice or behavior noted, in an audit, that breaches the requirements defined in the section **A.C.E.2.3. Code of Ethics and Professional Conduct** of this standard.

A.C.E.2.2. Audit Team Competence

A.C.E.2.2.1.1. The Service Provider shall ensure that individuals selected as audit team members in an audit engagement, possess the required competencies, as defined in the Appendix **6.2. Audit Team Competence Requirement**, to conduct the audit.

A.C.E.2.3. Code of Ethics and Professional Conduct

A.C.E.2.3.1. Impartiality and Independence

A.C.E.2.3.1.1. The Service Provider findings, conclusions and other work products may be leveraged by NCSA to enable assurance for a wide range of stakeholders. As a public interest matter, the Service Provider, its network firm, persons in charge with its governance and / or management, the audit team members, sub-contractors or partners shall be impartial and independent.

A.C.E.2.3.1.2. Impartiality and independence are closely linked, and in order for the Service Provider and the audit team members to be impartial in the audits related to NISCF's Services, they shall be in a state of independence from:

- The organization engaging the Service Provider;
- The applicant to NISCF Services;
- The organization(s) being audited and its scope; and
- The design, operation and maintenance of the activities subject to the audit.

A.C.E.2.3.1.3. The audit team members shall have independence of mind that permits the expression of conclusions without being affected by influences that compromise professional judgment, allowing every member to act with integrity, and exercise objectivity and professional skepticism.

A.C.E.2.3.1.4. The Service Provider, its network firms, persons in charge with its governance and / or management, the audit team members, sub-contractors or partners, shall have independence in appearance by

avoiding situations and / or relationships, that an informed third party, having knowledge of all relevant information, including the safeguards to independence applied, would reasonably conclude that the Service Provider or audit team members impartiality, integrity, objectivity or professional skepticism have been compromised.

A.C.E.2.3.1.5. Different situations, relationships or a combination of situations and relationships can result in impartiality or objectivity threats, and it is not possible to define or foresee all possible situations. Therefore, the Service Provider shall have professional independence and be responsible and accountable for its impartiality and objectivity, and of its audit team members, in relation with audit engagements and applicants to NISCF Services.

A.C.E.2.3.1.6. The Service Provider shall identify impartiality and independence risks, and enforce that the audit team members declare or report those risks related to their impartiality and independence, considering the below threats:

- Self-Interest;
- Self-Review;
- Endorsement, Involvement in governance and management, and Advocacy;
- Familiarity;
- Bias; and
- Intimidation.

A.C.E.2.3.1.7. When threats to impartiality and independence are identified, the Service Provider shall implement appropriate safeguards, if possible based on the situation(s) and relationship(s), that eliminate or mitigate the risks to impartiality and independence to reasonable and acceptable level.

A.C.E.2.3.1.8. When the Service Provider determines that appropriate safeguards are not available or cannot be applied to eliminate or mitigate the identified threats and risks to impartiality and independence, the Service Provider shall not accept or continue with the client and / or the audit engagement.

A.C.E.2.3.1.9. The Service Provider, its network firms, persons in charge with its governance and / or management, the audit team members, sub-contractors or partners, shall not conduct the below activities for an audit

client or related parties, as they constitute unmanageable threats to independence:

- Advisory, consultancy and implementation services related to the scope of an audit; and
- Internal audits, or activities that would result in detailed and technical recommendations related to the scope of an audit.

A.C.E.2.3.1.10. The Service Provider, its network firms, persons in charge with its governance and / or management, audit team members, sub-contractors or partners, shall not have the following relationships as they constitute unmanageable threats to independence:

- Controlling financially and / or legally, directly or indirectly, an audit client or related parties;
- Owning, totally or partially, through stocks, shares or any other forms of ownership, an audit client or related parties;
- Holding a significant credit over and / or being in debt to an audit client or related parties;
- Occupying a governance or management role and / or being appointed or contracted as special advisor, counselor or attorney to an audit client or related parties or persons in charge with their governance and / or management; and
- Having related individual(s), until fourth (4) degree of consanguinity or affinity, occupying a governance or management role and / or being appointed or contracted as special advisor, counselor or attorney to an audit client or related parties or persons in charge with their governance and / or management.

A.C.E.2.3.1.11. If the situations described in requirement **A.C.E.2.3.1.9** have occurred, or relationships described in requirement **A.C.E.2.3.1.10** existed, the Service Provider and / or the audit team member shall not engage or be part of an audit engagement with the audit client until a minimum period of three (3) years elapses since the end of involvement in the activities and / or relationships constituting the threat.

A.C.E.2.3.2. Objectivity and Integrity

A.C.E.2.3.2.1. The Service Provider and its audit team members shall act with integrity by being straightforward and honest in professional relationships.

A.C.E.2.3.2.2. Acting with integrity also implies that the Service Provider and its audit team members shall deal fairly with stakeholders, in full truthfulness.

A.C.E.2.3.2.3. Integrity also implies that the Service Provider and its audit team members shall not be associated with reports, returns, communications or other information where they believe that the information:

- Contains a materially false or misleading information;
- Contains statements or information furnished recklessly; or
- Omits or obscures information required to be included where such omission or obscurity would be misleading.

A.C.E.2.3.2.4. The Service Provider and its audit team members shall act with objectivity by not compromising professional or business judgment because of bias, conflict of interest or the undue influence of others.

A.C.E.2.3.2.5. The Service Provider and its audit team members shall avoid relationships that bias or unduly influence the professional judgment.

A.C.E.2.3.3. Professional Diligence and Skepticism

A.C.E.2.3.3.1. The Service Provider and its audit team members shall act diligently at all time.

A.C.E.2.3.3.2. The Service Provider shall always ensure full disclosure of risks and potential dangers of the audit to all stakeholders involved.

A.C.E.2.3.3.3. The Service Provider shall sufficiently research, investigate and learn about a new topics or updates before engaging in any audit that covers these topics.

A.C.E.2.3.3.4. The Service Provider shall only assign roles in audit engagements to audit team members that have evidenced that they have sufficient and appropriate competencies, based on the defined requirements in sections **A.C.E.2.1. Key Audit Roles** and **A.C.E.2.2. Audit Team Competence**.

A.C.E.2.3.3.5. Audit team members shall refrain from accepting assignments of audit tasks for which they feel they lack sufficient knowledge, experience, or technical expertise to perform effectively.

A.C.E.2.3.3.6. The Service Provider and its audit team members shall take part to audit in conformance with requirements defined in section **A.C.E.1.2. Proficiency**.

A.C.E.2.3.3.7. The audit team members shall ensure that they apply professional due diligence and care at all time through proper planning and constant monitoring of their actions and their implications.

A.C.E.2.3.3.8. The Service Provider and its audit team members shall continuously improve their knowledge and skills through training and professional development.

A.C.E.2.3.3.9. The Service Provider and its audit team members shall at all time follow the requirements defined in this standard and other relevant NISCF policies, standards, agreements, processes, procedures, terms and conditions related to the audit engagement.

A.C.E.2.3.3.10. The Service Provider and its audit team members shall also strive to follow other professional standards, when not contradicting with the requirements defined in this standard.

A.C.E.2.3.3.11. The Service Provider and its audit team members shall strive to provide high-quality and accurate reports, detailing findings, and recommendations.

A.C.E.2.3.3.12. The audit team members shall always apply professional skepticism through fact checking, evidence correlation and consultation with other audit team members.

A.C.E.2.3.3.13. The Service Provider and its audit team members shall always try to showcase to their client that they act diligently in following the audit principles defined in this standard.

A.C.E.2.3.4. Confidentiality

A.C.E.2.3.4.1. The Service Provider and its audit team members shall always and strictly abide by legal, regulatory and contractual confidentiality requirements and agreements.

A.C.E.2.3.4.2. The Service Provider and its audit team members shall maintain confidentiality and shall protect the privacy of clients and their data.

A.C.E.2.3.4.3. The Service Provider and its audit team members shall never disclose any confidential information about clients to any person, including the Service Provider employees who are unauthorized to access such information.

A.C.E.2.3.4.4. The Service Provider and its audit team members shall take precautionary measures to avoid unauthorized disclosure of confidential information.

A.C.E.2.3.4.5. The Service Provider and its audit team members shall only disclose audit information to any third-party after consent from the audit client (except for NCSA).

A.C.E.2.3.4.6. The Service Provider and its audit team members shall notify the client of the information related to the audit shared with NCSA.

A.C.E.2.3.4.7. The Service Provider and its audit team members shall collect, use, manage and protect information related to audit in accordance with the client data classification, labelling and security policies and other applicable laws and regulations.

A.C.E.2.3.4.8. If the Service Provider receives from the client sensitive information that is not intended to be used in the audit, the Service Provider shall communicate it to the client management such situation and destroy the shared information as per the client's procedures.

A.C.E.2.3.5. Other Professional Conduct Requirements

A.C.E.2.3.5.1. In relation with the other ethical values and professional behavior defined in this section **A.C.E.2.3. Code of Ethics and Professional Conduct**, the Service Provider and its audit team members shall:

- Use only software or process that is obtained legally and ethically;
- Always protect and respect the intellectual property requirements;
- Not engage in deceptive or improper financial practices and shall report any suspicion to the competent authorities;
- Report internally within the Service Provider, through escalations or whistleblowing channels, unethical or fraudulent practices or behavior;
- Always respect the scope boundaries of the engagement and shall log any violations committed;
- Ensure all audit activities are authorized by relevant stakeholders and within legal limits;
- Ensure that proper authorization and consent need to be obtained for the use of the client[4] systems and property;

[4] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

- Not associate with malicious hackers nor engage in any malicious activities;
- Not to take part in any black hat activity or be associated with any black hat community that serves to endanger others;
- Not make inappropriate reference to NCSA or misleading use of certificates, marks, logos or any other NISCF demarcation in publications, catalogues, documents, or talks;
- Not have been convicted in any felony or crime that could reasonably impair the Service Provider and its audit team members ability to provide audit services to clients;
- Uphold the reputation of the Cyber Security industry by adhering to recognized standards and best practices;
- Treat all parties with dignity and respect, regardless of their background, culture, or beliefs;
- Avoid discrimination or harassment of any kind; and
- Recognizing the importance of diversity and inclusion in the Cyber Security and audit industries.

A.C.E.3. Audit Technology

A.C.E.3.1. Computer-Assisted Audit Tools (CAATs)

A.C.E.3.1.1.1. The Service Provider shall ensure that the use of CAATs in an audit does not result in changes in the overall objectives and scope of work of the audit.

A.C.E.3.1.1.2. When using CAATs in an audit, the Service Provider shall have a clear understanding of the CAATs. This understanding shall be evidenced by:

- Documentation of the capabilities of the CAATs and the objective from their intended usage;
- Ability to understand and review the work to be performed by the CAATs;
- Demonstrating that the CAATs are compatible and can run effectively in the target technological environment; or
- Ability to understand and interpret the output(s) of the CAATs to build audit conclusions.

A.C.E.3.2. Artificial Intelligence (AI)

A.C.E.3.2.1.1. AI can be used in an audit, in multiple areas, like audit planning and resources optimization, risk assessment, data analytics, fraud detection, review automation. Other non-audit specific AI tools can also be leveraged by Auditors to assist in performing certain audit activities, like developing a testing procedure or creating templates. When using AI tools to conduct audit activities, the Service Provider shall ensure that the usage of AI tools considers national security guidelines for AI usage.

A.C.E.3.2.1.2. The Service Provider shall ensure that the results generated by AI tools used to perform audit activities are accurate, reliable, and in conformance with the desired outcomes.

A.C.E.3.2.1.3. The Lead Auditor shall review and validate the AI-generated results to maintain the quality and integrity of the Audit.

A.C.E.3.3. Robotic Process Automation (RPA)

A.C.E.3.3.1.1. In an audit, the Service Provider can create specific RPA tools for the audit or use standard RPA tools. In all cases, the Service Provider shall evidence that the results produced by the RPA are accurate.

A.C.E.3.3.1.2. The Service Provider shall validate manually, at least one transaction, for each audit testing procedure performed using an RPA tool.

A.C.E.3.4. Distributed Ledger Technology (DLT)

A.C.E.3.4.1.1. Distributed Ledger Technology (DLT) can be used to enhance the security and reliability of audit trails. When used in an audit, the Service Provider shall have clear documentation explaining the purpose, methods used and regulatory considerations for the development of DLT based audit tools.

A.C.E.3.4.1.2. The Service Provider shall have documented risks assessment for the use of DLT based audit tools and the related treatments and controls.

A.P. Audit Process

A.P.1. Client / Engagement Acceptance and Relationship Continuance

A.P.1.1. Engagement / Client Acceptance Due Diligence

A.P.1.1.1.1. The Service Provider shall document, before formally engaging with client, that it conforms with the requirements defined in sections **A.C.E.1.2. Proficiency** and **A.C.E.2.3.1. Impartiality and Independence**.

A.P.1.1.1.2. The Service Provider shall perform a review of the client's integrity and reputation, including its management.

A.P.1.1.1.3. The Service Provider shall contact the previous Service Provider engaged to identify and document any potential issues that could impact the delivery of the audit.

A.P.1.2. Engagement Preparation

A.P.1.2.1.1. The Service Provider shall sign a Non-Disclosure Agreement (NDA), with the client[5] before gaining access to any information related to the audit, unless these non-disclosure clauses are covered by the legally enforceable agreement defined in requirement **A.P.1.3.1.1**.

A.P.1.2.1.2. The Service Provider shall establish a secure communication channel with the client for further communications which ensures non-repudiation, authenticity, confidentiality, and integrity of the information communicated.

A.P.1.3. Formal Engagement Documentation

A.P.1.3.1.1. The Service Provider shall sign and ensure that the client signs, a legally enforceable agreement document for every audit engagement that serves as a contract between them, that shall include the following elements:

- Scope of work: A clear description of the audit services being provided, including any specific tasks, duration and deliverables;
- Scope(s) of audit(s): The exhaustive[6] listing of the Scope(s) of audit(s);

[5] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

[6] if the NISCF service requires NCSA acceptance of the scope prior to the audit and if available to the Service Provider at the time of contract drafting, the Service Provider can reference:

- Confidentiality: Confidentiality requirements governing the audit engagement;
- Termination: The circumstances under which the agreement can be terminated by either party;
- Governing law: The jurisdiction that will govern the agreement in case of any legal disputes (in the State of Qatar);
- Dispute resolution: A process for resolving any disputes that may arise during the audit engagement;
- Indemnification: A provision stating the conditions under which the Service Provider will indemnify the client against claims or damages resulting from the services provided;
- Liabilities: The liabilities limitations of the audit for the Service Provider;
- Client's responsibilities: The responsibilities of the client in relation to the audit engagement;
- Information sharing: A provision stating that the Service Provider may share specific information related to audit engagement with the National Cyber Security Agency (NCSA) in its capacity of the regulatory authority for Cyber Security domain;
- Changes to the scope of work: A provision for managing changes to the scope of work through performance of additional unplanned audits, required by NCSA or the client;
- Changes to the Scope(s) of audit(s): A provision for managing changes to the Scope(s) of audit(s), required by NCSA or the client, that impact the planned audits as part of the engagement and can require the performance of additional unplanned audits;
- A substitute (an Alternate) Service Provider: A provision for managing the liabilities and responsibilities of the engaged Service Provider in finding a substitute (an Alternate) Service Provider, if the Accreditation of the engaged Service Provider expires, is terminated or withdrawn during the engagement; and

---

- The unique identifier of the NISCF service request made by the client to NCSA; or
- The Scope Document and its version that was submitted by the client and accepted by NCSA.

- Terms and conditions: The terms and conditions under which the audit services will be provided.

A.P.1.3.1.2. The Service Provider shall ensure that legally enforceable agreement is signed by authorized signatories of the Service Provider and the client.

A.P.1.4. Engagement Communication

A.P.1.4.1.1. The Service Provider shall communicate to NCSA the engagement acceptance due diligence documentation as defined in section **A.P.1.1. Engagement Acceptance Due Diligence**, within five (5) working days[7] from the signature of legally enforceable agreement.

A.P.1.4.1.2. The Service Provider shall communicate to NCSA the legally enforceable agreement as defined in section **A.P.1.3. Formal Engagement Documentation**, within five (5) working days[8] from its signature.

A.P.1.4.1.3. The Service Provider shall request the appropriate and relevant information (please refer to section **A.P.7. Change (substitute) of Accredited Audit Service Provider**) from the previous Service Provider.

A.P.1.4.1.4. The Service Provider shall communicate to NCSA the relationship continuance confirmation documentation as defined in section **A.P.1.5. Relationship Continuance and Monitoring**, within five (5) working days[9] from its completion.

A.P.1.4.1.5. The Engagement Lead shall notify NCSA, in a timely manner, when the limitations described in requirement **A.C.E.1.5.1.4** could not be addressed in collaboration with the client.

A.P.1.5. Relationship Continuance and Monitoring

A.P.1.5.1.1. The Service Provider shall continuously monitor during an audit engagement that it continues to conform with the requirements defined in section **A.C.E.2.3. Code of Ethics and Professional Conduct**.

A.P.1.5.1.2. The Service Provider can be engaged to perform multiple audits as per of its contract (e.g., Follow-up audit, Maintenance or special audit(s)). Due to changes that could occur between audits, the Service Provider shall ensure that it still conforms with the requirements defined in sections **A.C.E.1.2. Proficiency**, **A.C.E.2.3.1. Impartiality and Independence** and

[7] Excluding National Holidays as declared by Emiri Diwan
[8] Excluding National Holidays as declared by Emiri Diwan
[9] Excluding National Holidays as declared by Emiri Diwan

reperform the client's integrity and reputation checks defined in requirement **A.P.1.1.1.2**, before the start of each audit.

A.P.2. Planning

A.P.2.1. Preliminary Work

A.P.2.1.1. Audit Objectives, Assertions, Period and Criteria

A.P.2.1.1.1. The Service Provider shall identify the audit objectives, that shall at least include the following:

- Determining the scope conformance to the audit criteria;
- Determining the ability of the subject of the audit (e.g., management system, process, system…) to enable client to conform with statutory, regulatory and contractual obligations[10];
- Determining the effectiveness of the subject of the audit in achieving its objectives; and
- If any, identify the Opportunities for Improvements (OFI).

A.P.2.1.1.2. When the audit objectives are defined by NCSA, through the NISCF Service, the Service Provider shall understand and adhere to these objectives.

A.P.2.1.1.3. When the audit objectives are defined by NCSA, through the NISCF Service, and the Service Provider and the client agreed to include additional objectives in the audit, the Service Provider shall ensure that these additional objectives do not impact negatively the objective defined by NCSA.

A.P.2.1.1.4. When circumstances described in requirement **A.P.2.1.1.3** occur, the Service Provider shall ensure that audit records are separately created and kept for each type of objectives (NCSA defined vs client defined).

A.P.2.1.1.5. The Service Provider shall identify and / or determine the audit assertions.

A.P.2.1.1.6. When assertions are determined by the audit criteria, the Service Provider shall ensure it considered all the audit assertions.

A.P.2.1.1.7. The Service Provider shall determine the audit period.

[10] NISCF Audit is not a legal compliance audit

A.P.2.1.1.8. The Service Provider shall clearly specify the audit criteria.

A.P.2.1.2. Environment Understanding

A.P.2.1.2.1. The Service Provider shall gain an understanding the organization(s) subject of the audit, through the analysis of at least:

- Its nature, operating model and organizational structure;
- Its objectives, strategy, values and principles;
- Its risk management, exposure and mitigation;
- Its relevant Cyber Security programs, frameworks and roles and responsibilities; and
- Its systems and technologies.

A.P.2.1.2.2. The Service Provider shall gain an understanding the organization(s) subject of the audit environment, through the analysis of at least:

- The main applicable laws, regulations and regulatory oversight;
- The industry and macro-environment; and
- The related entities.

A.P.2.1.3. Scope Review and Confirmation

A.P.2.1.3.1. The Service Provider shall review the scope in order to determine if:

- There are any restrictions to audit the defined scope;
- The underlying organizational, logical and physical boundaries described in the scope are complete and accurate;
- The systems and / or information assets related to the scope are complete and accurate; and
- The audit criteria, against which the scope will be audited, have been correctly and completely considered in the scope.

A.P.2.1.3.2. The Service Provider shall confirm that the scope has not been impacted by any significant changes, internal or external, since it was accepted by NCSA.

A.P.2.1.4. Preliminary Work Performance and Documentation

A.P.2.1.4.1. The Service Provider shall conduct the preliminary work activities prior to conducting plan preparation activities (please refer to section **A.P.2.2. Plan Preparation**).

A.P.2.1.4.2. The Service Provider shall document the conducted preliminary work activities and their results.

A.P.2.1.4.3. The Service Provider shall document and evidence that the results of the conducted preliminary work activities are taken into consideration in the next section **A.P.2.2. Plan Preparation**.

A.P.2.2. Plan Preparation

A.P.2.2.1. Audit Risk

A.P.2.2.1.1. The Service Provider shall start the preparation of the audit plan by conducting an audit risk assessment, based on a documented and approved audit risk assessment methodology, that conforms with the approach defined in this section.

A.P.2.2.1.2. The Service Provider shall determine the audit risk level using the assessed risk of material Non-Conformities (NC) and the detection risk.

A.P.2.2.1.3. The Service Provider shall start the audit risk assessment by identifying and assessing the inherent risk related to the scope, based on the results of the conducted preliminary work activities (please refer to section **A.P.2.1. Preliminary Work**).

A.P.2.2.1.4. The Service Provider shall assess the control risk related to the scope, based on the results of the conducted preliminary work activities (please refer to section **A.P.2.1. Preliminary Work**).

A.P.2.2.1.5. The Service Provider shall assess the risk of material Non-Conformities (NC) at the assertions level based on the assessed inherent risk and the control risk.

A.P.2.2.1.6. The Service Provider shall manage the detection risk in order to maintain the audit risk at a low acceptable level.

A.P.2.2.1.7. In reaching the required low acceptable level of the audit risk, the Service Provider shall evidence that it has considered:

- The expected confidence and reliance of the users of the audit report on the audit findings and conclusions; and
- The professional consensus on matters assessed during the audit risk assessment.

A.P.2.2.2. Audit Work Program

A.P.2.2.2.1. The Service Provider shall develop and document and audit work program that enables the audit team members to conduct all the audit activities required as per this standard (please refer to sections **A.P.2. Planning**, **A.P.3. Execution and Supervision**, **A.P.4. Reporting and Completion**, **A.P.5. Subsequent Events and Follow-up Activities** and **A.P.6. Maintenance, Special Audits and Re-Certification**) and other relevant NISCF standards specific to the NISCF's Service requiring the audit.

A.P.2.2.2.2. The Service Provider shall develop and document an audit work program that:

- Covers all the audit criteria;
- Serves the objectives of the audit (including the requirements set in the NISCF Service for which the audit is required); and
- Considers the audit period.

A.P.2.2.2.3. The Service Provider shall develop and document an audit work program that enable to evidence the conformance of the underlying subject(s) matter to audit criteria, for a defined audit period, on two audit conclusion levels:

- Design Effectiveness (DE); and
- Operating Effectiveness (OE).

A.P.2.2.2.4. The Service Provider shall develop and document an audit work program based on the detection risk required.

A.P.2.2.2.5. The Service Provider shall determine the nature of the audit procedures (please refer to requirement **A.P.3.1.2.6**) to be performed to ensure conformance of the underlying subject(s) matter to audit criteria.

A.P.2.2.2.6. The Service Provider shall plan for the testing of a specific assertion for a specific audit criterion using the adequate nature of the audit procedures.

A.P.2.2.2.7. The Service Provider shall determine the extent of the audit procedures to be performed to ensure conformance of the underlying subject(s) matter to audit criteria, in conformance with requirements defined in section **A.P.2.2.3**.

A.P.2.2.2.8. The Service Provider shall determine the timing of the audit procedures to be performed to ensure conformance of the underlying subject(s) matter to audit criteria.

A.P.2.2.2.9. When determining the extent and timing of the audit procedures, the Service Provider shall the working shifts of the organization(s) subject of the audit.

A.P.2.2.2.10. The Service Provider shall determine the detailed audit testing scripts to be performed in application of the nature, extent and timing of the audit procedures.

A.P.2.2.2.11. The Service Provider shall determine if there will be reliance on work performed by others during the audit.

A.P.2.2.2.12. The Service Provider shall document an audit work program that cover:

- The nature, extent and timing of the audit procedures;
- The audit testing scripts for each audit criteria;
- The underlying subject(s) matter for each audit criteria; and
- The access to person(s), site(s), system(s) and document(s) required to perform the audit procedures.

A.P.2.2.3. Audit Sampling

A.P.2.2.3.1. The Service Provider shall have and document a sampling methodology.

A.P.2.2.3.2. The Service Provider shall ensure that the selected sampling methodology shall be used in determining the extent of audit procedures, based on the detection risk required.

A.P.2.2.3.3. The Service Provider shall provide documented explanation, in the sampling methodology selected, of the extrapolation method and the related interpretation of sampling results.

A.P.2.2.3.4. Where the Scope(s) of audit(s) covers multiple sites, the Service Provider shall develop and document a sampling method that ensure proper and adequate audit of the scope.

A.P.2.2.3.5. When determining sample size, the Service Provider shall consider:

- Sampling risk;
- Tolerable error rate in the population; and
- Expected error rate in the sample.

A.P.2.2.3.6. The Service Provider shall verify that the population to be sampled is complete for the purpose of the audit procedure to be performed.

A.P.2.2.3.7. If the observed error rate in a sample exceeds the expected error rate in the sample, the Service Provider shall reassess the sampling risk to ensure that the deviation is not due to the sampling.

A.P.2.2.3.8. If the Service Provider finds that the sampling risk is unacceptable, it shall consider enlarging the extent of the audit procedures and increasing the sample size.

A.P.2.2.4. Use of the Work of Others

A.P.2.2.4.1. The Service Provider shall consider the use of the work of others in an audit, where appropriate.

A.P.2.2.4.2. When leveraging the work of others performed outside of the context of the audit (i.e., performed by other experts outside of the boundaries of the audit), the Service Provider shall assess the adequacy and completeness of the work of others with the audit objectives, assertions, period and criteria.

A.P.2.2.4.3. When the Service Provider decides to use the work of others during the audit (i.e., engaging other experts, for example technical experts, as part of the audit), it shall assess the adequacy of using work of others during audit planning by:

- Evaluating the independence and objectivity of the other experts that performed the work to be leveraged; and
- Assessing the proficiency, competencies, experience, resources of the other experts and the use of quality control procedure in their work.

A.P.2.2.4.4. When the Service Provider decides to use the work of others during the audit (i.e., engaging other experts, for example technical experts, as part of the audit), it shall gain an understanding of the scope of work, approach, timing and define the level of review necessary to be performed by the Service Provider over the work of others.

A.P.2.2.4.5. The Service Provider shall review the methodology, work program, work papers, final report and any other relevant deliverables of the other experts engaged during the audit, by assessing that their work was appropriately planned, supervised, documented and reviewed and determine the appropriateness and sufficiency of the audit evidence provided by them, and to which extent their work can be used and be relied on.

A.P.2.2.4.6. The Service Provider shall determine whether the work of others will be relied upon and incorporated directly or referred to separately in the audit findings.

A.P.2.2.4.7. The Service Provider shall determine the impact of the other experts' findings and conclusions on the audit objectives and assess if any additional work is required to achieve the audit objectives.

A.P.2.2.5. Audit Team Selection

A.P.2.2.5.1. The Service Provider shall select audit team members based on a documented procedure that shall:

- Allow for conformance with requirements defined in section **A.C.E.2.2. Audit Team Competence**; and
- Allow for conformance with relevant requirements defined in section **A.C.E.2.3. Code of Ethics and Professional Conduct**.

A.P.2.2.5.2. To determine the required audit team members, the Service Provider shall consider:

- Audit context (objectives, scope, criteria and deadlines);
- The competencies, knowledge and skills needed to achieve the objectives of the audit;
- Regulatory or contractual requirements;
- Language used to communicate with the client[11] and between audit team members; and
- Previous experience of the audit team members with the client and its systems or similar ones.

A.P.2.2.5.3. In consultation with audit team members (please refer to requirement **A.C.E.2.3.3.5**), the Lead Auditor shall assign to each audit team member, the responsibilities, he / she shall have during the audit.

A.P.2.2.5.4. When assigning tasks to audit team members, the Lead Auditor shall document that the assignment took into consideration:

- The competencies, knowledge and skills needed to conduct the audit activities assigned;
- The roles and responsibilities of non-audit team members (i.e., observers, interpreters and Technical Experts); and

[11] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

- The effective and efficient use of the audit team members selected.

A.P.2.2.6. Audit Calendar

A.P.2.2.6.1. The Service Provider shall determine the audit calendar based on a documented procedure that shall consider the:

- Audit criteria;
- Size, context and complexity of the client[12];
- Laws and regulatory requirements;
- In-house and outsourced activities within the scope;
- Previous audit findings;
- Sites to be audited;
- Audit risk assessment results; and
- Audit team composition.

A.P.2.2.6.2. The Service Provider shall record the justification of the audit calendar.

A.P.2.2.7. Audit Tools

A.P.2.2.7.1. The Service Provider shall determine and record the audit technology and tools that will be used during the audit to gather evidence, perform tests and reporting.

A.P.2.2.7.2. The Service Provider shall document conformance with relevant requirements defined in section **A.C.E.3. Audit Technology**.

A.P.2.3. Plan Documentation

A.P.2.3.1.1. The Service Provider shall document an audit plan that shall at least include or reference to:

- Audit objectives;
- Audit assertions;
- Audit period;

[12] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

- Audit criteria;
- Audit scope;
- Audit Calendar, including the audit procedures timing if required to be communicated to the client[13];
- Sites to be audited;
- Interviews plan;
- External confirmation list;
- Information / documents request list;
- Audit team composition and other observers, interpreters and Technical Experts; and
- Deliverables, their audience and their usage.

A.P.2.4. Plan Communication

A.P.2.4.1.1. The Service Provider shall communicate the audit plan to the client[14], sufficiently in advance to allow the client to grant the required accesses on time.

A.P.2.4.1.2. The Service Provider shall communicate the audit plan to NCSA prior to the start of the execution of the audit as defined in section **A.P.3. Execution and Supervision**.

A.P.2.4.1.3. The Service Provider shall communicate to NCSA, along with the audit plan:

- The audit risk assessment results;
- The audit work program; and
- The audit sampling methodology, if applicable.

A.P.2.4.1.4. The Lead Auditor shall communicate to the rest of audit team members, the audit tasks that are assigned to them.

[13] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.
[14] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

A.P.3. Execution and Supervision

A.P.3.1. Audit Activities Performance

A.P.3.1.1. Kick-Off

A.P.3.1.1.1. The Lead Auditor shall organize and record a kick-off meeting with the client[15] management, if possible, those for the processes, systems and departments to be audited.

A.P.3.1.1.2. The Lead Auditor shall cover during the kick-off meeting the following aspects:

- Presentation of the audit team composition and other observers, interpreters and Technical Experts and their roles in the audit;
- Confirmation of the audit scope;
- Presentation of the audit plan;
- Agreement on dates of progress and completion meetings;
- Confirmation of the channels that will be used for communication between the audit team and the client, including the language used and reporting rules;
- Presentation of the needed resources by the audit team from the client and confirmation of their availability;
- Collection and acknowledgement of security, emergency and safety procedures that the audit team needs to comply with;
- Confirmation of reporting methods;
- Presentation of the potential situations under which the audit can be prematurely closed or put-on-hold;
- Reminder that the audit team members representing the Service Provider are responsible for the plan and execution of audit activities;
- Confirmation of the status of previous Non-Conformities (NC), if any; and
- Methods, procedures and tools that will be used for sampling.

[15] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

A.P.3.1.1.3. The Service Provider shall invite NCSA to attend the Kick-Off meeting at least five (5) working days[16] before the meeting date.

A.P.3.1.2. Audit Evidence

A.P.3.1.2.1. The Service Provider shall obtain sufficient and appropriate evidence, to form a reasonable basis for the audit findings and conclusions.

A.P.3.1.2.2. The Service Provider shall collect relevant and reliable evidence[17].

A.P.3.1.2.3. The Service Provider shall use only verifiable evidence.

A.P.3.1.2.4. When the Service Provider is unable to collect audit evidence by its own resources or through independent source (e.g., Information Produced by the Client[18] (IPC)), the Service Provider shall assess if the evidence provided is sufficient and appropriate by collecting additional evidence that verify the completeness and accuracy of the IPC.

A.P.3.1.2.5. The Service Provider shall determine the appropriate audit procedures to be used to collect sufficient and appropriate evidence when conducting different audit activities (i.e., risk assessment, compliance testing or substantive testing).

A.P.3.1.2.6. The Service Provider shall consider the following types of audit procedures for evidence collection and production:

- Inquiry;
- Confirmation;
- Observation;
- Inspection;
- Analytical procedure;
- Precomputation /Reperformance; and / or

[16] Excluding National Holidays as declared by Emiri Diwan.
[17] The relevance of audit evidence is linked to the assertion or to the objective of the control being tested. The reliability of audit evidence is linked to the nature and source of the audit evidence and the circumstances under which it was obtained, taking into consideration the knowledge level of the source, its independence, the level of control over the information and the collection method.
[18] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

- Other professionally accepted methods[19].

A.P.3.1.2.7. The Service Provider shall record and keep clear identification of the evidence supporting findings.

A.P.3.1.2.8. When an Auditor has doubts about the reliability of audit evidence, he / she shall report the fact to the Lead Auditor, who shall corroborate evidence from multiple sources to determine the required actions.

A.P.3.1.2.9. When the Service Provider is unable to obtain appropriate and sufficient audit evidence, it shall report the matter to client in order to overcome the issue.

A.P.3.1.3. Audit Documentation

A.P.3.1.3.1. The Service Provider shall have standardized working papers that are designed to record all the necessary information required to perform and report on the planned audit activities.

A.P.3.1.3.2. The Service Provider shall document all audit activities conducted defined in this standard.

A.P.3.1.3.3. The Service Provider shall produce and maintain evidence of its compliance with relevant audit standards requirements, including this standard.

A.P.3.1.3.4. The Service Provider shall ensure that the audit documentation contain sufficient information to enable another auditor, who does not have any previous connection with the audit:

- To understand the objectives, assertions, period and criteria;
- To gain knowledge of the preliminary work conducted and its impact on the plan preparation;
- To understand the audit risk assessment of the Service Provider and nature, extent and timing of the audit procedures, as well as their results;
- To understand the evidence gathered and the findings and conclusions; and
- To determine the auditor that performed the work and its review.

[19] These methods are not generally used and may requires approvals from the client before applying them (e.g., social engineering…)

A.P.3.1.3.5. The Service Provider shall ensure that documentation of audit procedures shall clear record:

- The individual(s) interviewed and their claims;
- The confirmation(s) collected and their means;
- The time and place of observation(s) made as well as the witnesses;
- The document(s), record(s) and other information media(s) inspected;
- The information and element(s) used for the analytical procedures, precomputation and reperformance; and
- The audit testing scripts.

A.P.3.1.3.6. The Service Provider shall document adequately, and if necessary separately, significant matters related to the audit.

A.P.3.1.3.7. The Service Provider shall store the audit documentation, including the audit evidence, in a secure and encrypted format.

A.P.3.1.3.8. The Service Provider shall ensure that access to audit documentation, including evidence, is limited and on a need-to-know basis.

A.P.3.1.3.9. The Service Provider shall retain all the audit documentation for three (3) years after the end of the relationship with the client.

A.P.3.1.4. Design Effectiveness (DE) Audit

A.P.3.1.4.1. The Service Provider shall perform Design Effectiveness (DE) audit activities to:

- Verify the design, documentation, approval and communication to relevant parties of required documentation as per the audit criteria;
- Evaluate the client[20] site(s) specificities;
- Determine the preparedness for the Operating Effectiveness (OE) audit; and
- Ensure the client's understanding and adoption of the standard(s) defining the audit criteria.

[20] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

A.P.3.1.4.2. Inquiries is a Design Effectiveness (DE) audit procedure, and the Service Provider shall not solely rely on inquiries for the Design Effectiveness (DE) audit.

A.P.3.1.4.3. If there are any significant changes that would impact the scope, between the performance of the Design Effectiveness (DE) audit and the Operating Effectiveness (OE) audit, the Service Provider shall consider the necessity to reperform the Design Effectiveness (DE) audit before starting the Operating Effectiveness (OE) audit.

A.P.3.1.5. Operating Effectiveness (OE) Audit

A.P.3.1.5.1. The Service Provider shall perform Operating Effectiveness (OE) audit activities to:

- Verify the implementation and effective conformity of the controls, systems and processes to the audit criteria;
- Ensure that the defined performance objectives of the processes and controls are met;
- Verify the ability of meeting statutory, regulatory and contractual obligations; and
- Confirm the internal audit and management responsibilities and reviews.

A.P.3.1.5.2. The Service Provider shall ensure that the Operating Effectiveness (OE) audit covers the audit period.

A.P.3.1.5.3. The Service Provider shall perform the Operating Effectiveness (OE) audit on-site.

A.P.3.1.5.4. When the on-site Operating Effectiveness (OE) audit is performed virtually, the Service Provider shall have specific rules to ensure the virtual delivery does not impact the audit.

A.P.3.1.6. Findings and Conclusions

A.P.3.1.6.1. The Service Provider shall record findings that justify in details the conclusion for each audit criterion.

A.P.3.1.6.2. The Service Provider shall record findings that clearly provide the rationale of the conformity or not of the underlying subject(s) matter to the audit criterion.

A.P.3.1.6.3. The Service Provider shall record findings that identify in detail the evidence on which the conclusion is based.

A.P.3.1.6.4. The Service Provider shall provide a conclusion for each audit criterion at the two audit conclusion levels, unless not applicable or deemed impractical:

- Design Effectiveness (DE); and
- Operating Effectiveness (OE).

A.P.3.1.6.5. The Service Provider shall provide conclusion at each audit conclusion level based on the below classification:

- Conformity;
- Conformity with Opportunities for Improvements (OFI); and
- Non-Conformity.

A.P.3.1.6.6. When using sampling, the Service Provider shall determine, through extrapolation, if the potential errors in the entire population (projected error rate) exceeds the tolerable error rate.

A.P.3.1.6.7. The Service Provider shall always conclude as a Non-Conformity, a control or process with errors or exceptions when they have been overridden by management resulting in fraud or illegal acts.

A.P.3.2. Audit Supervision

A.P.3.2.1. Monitoring and Adjustments

A.P.3.2.1.1. The Lead Auditor shall track the audit progress as per the audit plan.

A.P.3.2.1.2. The Service Provider shall update the audit plan, if there is any change impacting the information contain on it as defined in the requirements of section **A.P.2.3. Plan Documentation**.

A.P.3.2.1.3. The Service Provider shall monitor during the audit conformance with the requirements defined in section **A.C.E.2.3. Code of Ethics and Professional Conduct**, and take the appropriate actions if deviations are observed.

A.P.3.2.1.4. The Service Provider shall assess, after the Design Effectiveness (DE) audit, if the risk of material Non-Conformities (NC) and detection risk (please refer to section **A.P.2.2.1. Audit Risk**) shall be adjusted.

A.P.3.2.1.5. Based on the reporting of Design Effectiveness (DE) findings and conclusions to the client[21] (please refer to requirement **A.P.4.1.1.1**), and in the light of the client's decision to address the identified Non-Conformities (NC) before the Operating Effectiveness (OE) audit, the Service Provider shall determine and record:

- Changes to the audit plan, including the postponement of the Operating Effectiveness (OE) audit;
- The impact of such changes on the reasonable expectation (please refer to requirement **A.C.E.1.5.1.2**) to continue and complete the audit in conformance with the NISCF policies, standards, processes, terms and conditions, specific to the NISCF's Service requiring the audit; and
- If in cases where the Design Effectiveness (DE) audit showcase clearly that the client is not, and would probably be not, ready for the Operating Effectiveness (OE) audit, the explanation and justification of such situation.

A.P.3.2.1.6. If the adjustments described in requirement **A.P.3.2.1.4** are introduced, the Service Provider shall determine and perform the other necessary adjustments to the plan.

A.P.3.2.1.7. The Service Provider shall monitor the performance of the audit work program and determine if adjustment shall be introduced.

A.P.3.2.1.8. The Engagement Lead shall determine performance criteria for the Lead Auditor and Auditors and assess their performance during the audit.

A.P.3.2.1.9. The Service Provider shall make the necessary adjustments to the audit team members based on the performance review described in requirement **A.P.3.2.1.8**.

A.P.3.2.1.10. While the Service Provider is not expected to have extensive expertise in document authentication, the Service Provider shall adjust its planned audit procedures or perform additional audit procedures when it detects that shared documents by the client were not authentic.

A.P.3.2.2. Findings and Conclusions Review and Confirmation

[21] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.

A.P.3.2.2.1. The Service Provider shall ensure that Non-Conformities (NC), exceptions and errors are discussed with the processes and controls owners to make sure that the findings are understood and supported by accurate evidence.

A.P.3.2.2.2. The Lead Auditor shall:

- Assess based on the audit objectives, assertations and criteria if the findings and supporting the evidence are correctly recorded by the auditors;
- Build agreed-on audit conclusions among the audit team;
- Identify, record and present to the auditor any follow-up actions to be performed; and
- Review the audit work program, in the light of the findings, to ensure if the audit activities performed are adequate and sufficient.

A.P.3.2.2.3. When Non-Conformities (NC) have been identified and if compensating controls exist, the Service Provider shall report the specific audit criterion that was assessed with a Non-Conformity, as:

- Non-Conformity when the compensating controls are ineffective; or
- Conformity, when the compensating controls are fully effective and the Service Provider shall provide explanation and justification of how the compensating controls address the Non-Conformities (NC).

A.P.4. Reporting and Completion

A.P.4.1. Intermediate Reporting

A.P.4.1.1.1. The Service Provider shall report to the client[22] the Design Effectiveness (DE) findings and conclusion.

A.P.4.1.1.2. The Service Provider shall report the Design Effectiveness (DE) findings and conclusions, using defined NCSA reporting tools if available, to NCSA within five (5) working days[23] from the completion of the Design Effectiveness (DE) activities.

[22] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.
[23] Excluding National Holidays as declared by Emiri Diwan

A.P.4.2. Completion

A.P.4.2.1.1. The Lead Auditor shall organize and record a formal completion meeting, with the client[24] management, if possible, those for the processes, systems and departments to audited.

A.P.4.2.1.2. The Lead Auditor shall cover during the completion meeting the following aspects:

- Presentation that the evidence collected can be based on a sample and therefore introducing an element of uncertainty;
- Presenting and validating all findings;
- Reminder of the method of reporting required by this standard and the timeframe for the final report; and
- Collect information on the timeframe necessary for the client to present a Corrective Actions Plan (CAP) for Non-Conformities (NC) reported.

A.P.4.2.1.3. The Service Provider shall give the opportunity during the completion meeting discussion the findings and conclusions and ask the needed questions.

A.P.4.2.1.4. The Lead Auditor shall attempt to resolve any disagreement with client regarding audit evidence, findings and conclusions.

A.P.4.2.1.5. Based on the output of requirement **A.P.4.2.1.4**, the Service Provider shall record all the unresolved points.

A.P.4.2.1.6. The Service Provider shall invite NCSA to attend the completion meeting at least five (5) working days[25] before the meeting date.

A.P.4.2.1.7. Before incorporating Corrective Actions Plan (CAP) of the client in the audit report (please refer to requirement **A.P.4.3.1.4**), the Service Provider shall ensure that the CAP clearly include the following elements:

- Detailed corrective activities to resolve the Non-Conformities (NC), errors or exceptions identified during the audit and their correction, including a root-cause analysis;

[24] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant.
[25] Excluding National Holidays as declared by Emiri Diwan

- The implementation timeline;
- The individual / function responsible for the corrective activities and corrections; and
- If it is not practically or chronologically feasible to implement corrective activities, details of activities to build preventive controls that have for aim to prevent the re-occurrence of the Non-Conformities (NC), errors or exceptions.

A.P.4.3. Final Reporting

A.P.4.3.1.1. The Service Provider shall report to the client[26] the findings and conclusions, using defined NCSA reporting tools if available, to NCSA on Design Effectiveness (DE) and Operating Effectiveness (OE) and a draft of the audit report, with the invitation to attend the completion meeting (please refer to requirement **A.P.4.2.1.6**).

A.P.4.3.1.2. The Service Provider shall report the final[27] findings and conclusions, using defined NCSA reporting tools if available, to NCSA on Design Effectiveness (DE) and Operating Effectiveness (OE) within ten (10) working days[28] from the completion meeting date, if no Non-Conformities (NC) have been reported, or within ten (10) working days[29] from the communication of the Corrective Actions Plan (CAP), if Non-Conformities (NC) have been reported.

A.P.4.3.1.3. The Service Provider shall provide to NCSA and the client, within the same timeline defined in requirement **A.P.4.3.1.2**, a clearly dated final audit report signed by an authorized signatory of the Service Provider.

A.P.4.3.1.4. The audit report shall include:

- A clear title that distinguish the report from any other potential reporting that is not governed by this standard;
- An introduction that details:

---

[26] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant

[27] The findings and conclusions in the final reporting shall be updated, if based on the completion meeting, there is agreement with client to change findings or conclusions, or based on NCSA review and instruction of the Design Effectiveness (DE) and Operating Effectiveness (OE) shared in conformance with requirement A.P.4.3.1.1.

[28] Excluding National Holidays as declared by Emiri Diwan

[29] Excluding National Holidays as declared by Emiri Diwan

i. Clear identification of the Service Provider, including its Accreditation identification;

ii. Clear identification of the client, including address, legal or commercial identifier;

iii. The type of the audit (e.g., initial, maintenance…);

iv. Audit objectives, assertions, period and criteria; and

v. The recipients of the report as required by this standard and according to the terms of engagement.

- An audit history:

i. The dates and places in which the audit activities were conducted;

ii. The audit team members and other participants to the audit and their role;

iii. The key individual(s) that have been interviewed or consulted for the purpose of the audit;

iv. The observed deviations from the communicated audit plan and the related justification; and

v. Issues, restrictions or limitations encountered during the audit, especially those impacting the performance of the audit work program.

- Detailed reporting for all audit criteria:

i. Findings and conclusions for both Design Effectiveness (DE) and Operating Effectiveness (OE) aligned with findings and conclusions provided in the reporting tools;

ii. Reference to evidence used;

iii. Identification of the underlying subject(s) matter that included Non-Conformities (NC), errors or exceptions;

iv. Generic[30] recommendation from the Service Provider to address the Non-Conformities (NC) and Opportunities for Improvements (OFI) reported; and

v. The client Corrective Actions Plan (CAP), including the Service Provider's assessment of the CAP for newly reported Non-Conformities (NC) and the effectiveness of corrective actions regarding Non-Conformities (NC) reported in previous audit(s).

- Other Significant Matters:

i. Significant changes to the scope since it was approved by NCSA or the last audit;

ii. Disclaimer related to the sampling risks and information availability; and

iii. Confirmation that the audit objectives were achieved and that the scope validity.

A.P.4.4. Other Reporting

A.P.4.4.1.1. The Service Provider shall respond to all specific Clarification and Evidence Request(s) from NCSA in the format and timeline instructed by NCSA.

A.P.4.4.1.2. When the issues described in requirement **A.P.3.1.2.9** are not resolved with the help of the client, and if in the Service Provider judgment the situation would lead to the inability to maintain the audit risk at a low acceptable level, the Service Provider shall report the matter to NCSA with a clear description of the situation and evidence that it is impractical to reduce the detection risk through other means.

A.P.4.4.1.3. When the Service Provider identified any of the situations described in requirement **A.P.2.1.3.1** or changes described in requirement **A.P.2.1.3.2**, it shall, without undue delays, reported them to NCSA and the client.

A.P.4.4.1.4. The Service Provider shall report to the client[31] all identified errors or exceptions (including controls on which minimal design flaws or operating

[30] Guidance or detailed instruction on how the address the Non-Conformities (NC) and Opportunities for Improvements (OFI), that could reasonably be considered as advise shall not be provided.

[31] The use of the term "client" in this section refers to the applicant to NISCF Service, and the organization(s) being audited if legally different from the applicant

deviation or have been identified but still assessed and reported as Conformity).

A.P.4.4.1.5. The Service Provider shall report the progress on the audit to the client as per the agreed-on communication schedule.

A.P.4.4.1.6. When significant changes are introduced to the audit (please refer to requirements defined in section **A.P.3.2.1. Monitoring and Adjustments**), the Service Provider shall share with NCSA, without undue delays, the updated versions of the audit documentation, that are required to be shared with NCSA as per this standard and other NISCF policies, standards, processes, terms and conditions, specific to the NISCF's Service requiring the audit, especially changes related to the audit work program, audit calendar and changes described in requirements **A.P.3.2.1.5** and **A.P.3.2.1.9**.

A.P.5. Subsequent Events and Follow-up Activities

A.P.5.1.1.1. The Service Provider shall inquire with the client as to whether there are any subsequent events[32], that could have a material effect on the audit report.

A.P.5.1.1.2. In such situation, the Service Provider shall present in the audit report, in a clearly distinctive section, a description of the events, the consequences (verified or potential) on the scope, the findings and conclusions of the audit.

A.P.5.1.1.3. The Service Provider could be requested by NCSA to perform follow-up activities after the completion of the audit and submission of the audit report. Therefore, the Service Provider shall perform the follow-up activities. These activities can be due to:

- The need to verify the corrective actions effectiveness; or
- The need to perform audit activities that were not performed by the Service Provider or reperform audit activities that were performed by the Service Provider but not appropriately documented.

A.P.6. Maintenance, Special Audits and Re-Certification

A.P.6.1. Relationship Continuance Confirmation

[32] Events occurring between the completion meeting date and the audit report issuance date

A.P.6.1.1.1. Prior to the start of any subsequent audit (i.e., after the initial audit), the Service Provider shall conduct the relationship continuance and monitoring checks defined in requirement **A.P.1.5.1.2**.

A.P.6.1.1.2. The Service Provider shall communicate to NCSA the evidence of the confirmation of the relationship continuance with the client as per the requirement **A.P.1.4.1.4**.

A.P.6.2. Rest of Audit Process

A.P.6.2.1. Planning

A.P.6.2.1.1. The Service Provider shall identify the audit objectives, assertions, period and criteria depending on the audit (i.e., maintenance, scope expansion, suspension, other special audit(s) or re-certification) (please refer to section **A.P.2.1.1. Audit Objectives, Assertions, Period and Criteria**).

A.P.6.2.1.2. Unless specified in the NISCF Service requirements for which the audit is required, the Service Provider shall set the following objectives for the different audit(s):

- Maintenance: The objective is to confirm whether or not, the Non-Conformities (NC) reported in the previous audit were addressed and that changes occurred to the subject of the audit (e.g., management system, process, system…), if any, are in Conformity with the audit criteria;
- Suspension: The objective is to confirm that whether or not, the Corrective Actions Plan (CAP) and its implementation address effectively, the Non-Conformities (NC) that led to the suspension;
- Scope Expansion: Similar to the initial audit, the objective is to confirm whether or not, the scope is compliant (based on the defined requirements) but only for the expansion;
- Other special audit(s): The Objective is defined by NCSA; and
- Re-certification: Similar to the initial audit, the objective is to confirm whether or not, the scope is compliant (based on the defined requirements) for the entire scope. The difference is during Re-Certification the objective is also to confirm whether or not, the Non-Conformities (NC) reported in the previous audit were addressed and that changes occurred to the subject of the audit (e.g., management system, process, system…), if any, are in Conformity with the audit criteria.

A.P.6.2.1.3. In defining the audit criteria during a maintenance, the Service Provider shall cover:

- The audit criteria for which Non-Conformities (NC) were reported in the previous audit; and
- The audit criteria that would require to be audited for the changes occurred to the subject of the audit (e.g., management system, process, system…).

A.P.6.2.1.4. In defining the audit criteria during a special audit related to scope expansion, the Service Provider shall consider:

- The audit criteria for the existing scope and their applicability to the expansion; and
- The audit criteria specific to the expansion.

A.P.6.2.1.5. In defining the audit criteria during a special audit related to suspension, the Service Provider shall consider the audit criteria for which Non-Conformities (NC) that led to the suspension.

A.P.6.2.1.6. In defining the audit criteria during a Re-Certification audit, the Service Provider shall consider all the audit criteria for the latest existing scope.

A.P.6.2.1.7. The Service Provider shall confirm the audit environment and scope understanding (please refer to sections **A.P.2.1.2. Environment Understanding** and **A.P.2.1.3. Scope Review and Confirmation**) it built, continues to be relevant to base the audit on.

A.P.6.2.1.8. The Service Provider shall document the Preliminary Work for the audit in conformance with the requirements defined in section **A.P.2.1.4. Preliminary Work Performance and Documentation**.

A.P.6.2.1.9. The Service Provider shall conduct an audit risk assessment for the audit in conformance with requirements defined in section **A.P.2.2.1. Audit Risk**.

A.P.6.2.1.10. Based on the audit criteria for the audit (please refer to requirement **A.P.6.2.1.3**, **A.P.6.2.1.4**, **A.P.6.2.1.5** or **A.P.6.2.1.6**) and taking into consideration the relevant levels for the audit (please refer to requirement **A.P.2.2.2.3**) and the requirements defined by the NISCF Service which requires the audit (please refer to requirement **A.P.2.2.2.2** second (2) indentation), the Service Provider shall document, in conformance with requirement **A.P.2.2.2.12**, the audit work program that shall conform to the relevant requirements (i.e., from **A.P.2.2.2.3** to **A.P.2.2.2.11**).

A.P.6.2.1.11. The Service Provider shall prepare the audit plan of the audit in conformance with requirements defined in sections **A.P.2.2.3. Audit Sampling**, **A.P.2.2.4. Use of the Work of Others**, **A.P.2.2.5. Audit Team Selection**, **A.P.2.2.6. Audit Calendar** and **A.P.2.2.7. Audit Tools**.

A.P.6.2.1.12. The Service Provider shall document the audit plan of the audit in conformance with requirements defined in section **A.P.2.3. Plan Documentation**.

A.P.6.2.1.13. The Service Provider shall communicate the audit plan of the audit in conformance with requirements defined in section **A.P.2.4. Plan Communication**.

A.P.6.2.2. Execution and Supervision

A.P.6.2.2.1. The Service Provider shall execute and supervise the audit in conformance with requirements defined in section **A.P.3. Execution and Supervision**.

A.P.6.2.3. Reporting

A.P.6.2.3.1. The Service Provider shall conduct the audit completion activities in conformance with requirements defined in section **A.P.4.2. Completion**.

A.P.6.2.3.2. The Service Provider shall perform reporting on the audit in conformance with the requirements defined in section **A.P.4.3. Final Reporting**.

A.P.6.2.3.3. For scope expansion and re-certification audit(s), the Service Provider shall perform intermediate reporting in conformance with the requirements defined in section **A.P.4.1. Intermediate Reporting**.

A.P.6.2.3.4. During an audit, the Service Provider shall ensure that any reporting required as defined in section **A.P.4.4. Other Reporting**, is performed in conformance with these requirements.

A.P.7. Change (substitute) of Accredited Audit Service Provider

A.P.7.1.1.1. In the event that the Service Provider is unable to complete the audit engagement for any reason and the client engages an alternate Service Provider, the former must, upon request, share the necessary information with the appointed Auditor.

A.P.7.1.1.2. The Service Provider shall provide the appointed Service Provider (alternate) with, at minimum, the following information:

- All the reporting made to the client and NCSA during the engagement;

- Documentation requested and gathered regarding the Corrective Action Plan (CAP);
- List of documents requested and collected; and
- Details of interviews conducted.

5. Compliance and Enforcement

5.1. Compliance Process

All applicants to NISCF's Audit Accreditation Services and Accredited Audit Service Providers by NCSA 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

New NISCF Certification requests shall conform with this standard 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 standard.

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 requirements 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 Audit Accreditation Services and Accredited Audit 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

AI	Artificial Intelligence.
CAAT	Computer-Assisted Audit Tool.
CAP	Corrective Actions Plan.
DE	Design Effectiveness.
DLT	Distributed Ledger Technology.
IPC	Information Produced by the Client.
IQCR	Independent Quality Control Reviewer.
NC	Non-Conformities.
NCGAA	National Cyber Governance and Assurance Affairs.
NCSA	National Cyber Security Agency.
NDA	Non-Disclosure Agreement.
NISCF	National Information Security Compliance Framework.
OE	Operating Effectiveness.
OFI	Opportunities for Improvements.
RPA	Robotic Process Automation.

6.2. Audit Team Competence Requirement

The competence criteria specify the knowledge and skills that the Service Provider's Audit Accreditation Service Team shall have for each role in the Audit Accreditation Services activities. The organization shall evaluate its Accreditation Service Team based on these criteria.

Required Competency		Audit Team Roles		
Reference	**Knowledge and Skills**	**Engagement Lead**	**Lead Auditor**	**Auditor**
General				
C.AUD.G.1	Knowledge of the client's business and sector (the competency assessment shall specify which industry the personnel has knowledge of)	X	X	X
C.AUD.G.2	Knowledge of capability and capacity management	X	X	
C.AUD.G.3	Knowledge of risk assessment and management methodologies	X	X	
C.AUD.G.4	Knowledge of information security controls and their objectives	X	X	
C.AUD.G.5	Knowledge of confidentiality protection best practices	X	X	X
C.AUD.G.6	Knowledge of escalation protocols		X	X
C.AUD.G.7	Project management skills	X	X	
C.AUD.G.8	Communication and leadership skills	X	X	
C.AUD.G.9	Resources and team management skills	X	X	
C.AUD.G.10	Problem management skills	X	X	
C.AUD.G.11	Negotiation skills	X	X	

Required Competency		Audit Team Roles		
Reference	**Knowledge and Skills**	**Engagement Lead**	**Lead Auditor**	**Auditor**
C.AUD.G.12	Presentation skills	X	X	X
C.AUD.G.13	Finding summarizing and drafting skills		X	X
C.AUD.G.14	Reporting skills		X	X
C.AUD.G.15	Note taking skills			X
C.AUD.G.16	Interviewing skills		X	X
C.AUD.G.17	Fact checking skills		X	X
C.AUD.G.18	Physical and Electronic documents authentication skills		X	X
C.AUD.G.19	Tasks assignment and monitoring skills	X	X	
Service Delivery: Audit Service				
C.AUD.SD.1	Knowledge of audit principles	X	X	X
C.AUD.SD.2	Knowledge of the industry standards and regulations related to audit, including Ethics and Code of Conduct	X	X	X
C.AUD.SD.3	Knowledge of cyber / information security risks	X	X	X
C.AUD.SD.4	Knowledge of legal and contractual tools related to audit	X	X	
C.AUD.SD.5	Knowledge of audit methodologies	X	X	X
C.AUD.SD.6	Knowledge of audit engagement stakeholders and their roles and responsibilities	X	X	
C.AUD.SD.7	Knowledge of common IT / OT systems and protocols		X	X
C.AUD.SD.8	Knowledge of common IT infrastructure and network assets		X	X

Required Competency		Audit Team Roles		
Reference	**Knowledge and Skills**	**Engagement Lead**	**Lead Auditor**	**Auditor**
C.AUD.SD.9	Knowledge of the main Cyber Security standards and frameworks		X	X
C.AUD.SD.10	Knowledge of main business processes, organizational structures and operating models		X	
C.AUD.SD.11	Knowledge of main automated or computer assisted audit tools and techniques		X	X
C.AUD.SD.12	Knowledge of audit risk concepts		X	X
C.AUD.SD.13	Knowledge of the nature of audit procedure		X	X
C.AUD.SD.14	Knowledge of sampling methodologies		X	
C.AUD.SD.15	Knowledge of main Cyber Security / IT Certification, Attestations and other assurance mechanisms		X	
C.AUD.SD.16	Knowledge of audit evidence recording techniques		X	X
C.AUD.SD.17	Knowledge of audit documentation securing techniques		X	X
C.AUD.SD.18	Knowledge of internal audit department duties and responsibilities		X	X
C.AUD.SD.19	Knowledge of engagement closure practices	X	X	
C.AUD.SD.20	Knowledge of NISCF relevant policies, standards and procedures	X	X	X
C.AUD.SD.21	Knowledge of the audit criteria of main NCSA's Information Security standard and framework and international best practices	X	X	X

Required Competency		Audit Team Roles		
Reference	**Knowledge and Skills**	**Engagement Lead**	**Lead Auditor**	**Auditor**
C.AUD.SD.22	Engagement acceptance due diligence and risk management skills	X	X	
C.AUD.SD.23	Audit scoping skills, including the selection of the adequate approach and controls	X	X	
C.AUD.SD.24	Planning skills		X	X
C.AUD.SD.25	Audit risk assessment skills		X	
C.AUD.SD.26	Underlying subject(s) matter identification skills		X	X
C.AUD.SD.27	Sampling selection skills		X	X
C.AUD.SD.28	Planning documentation referencing and correlation skills		X	
C.AUD.SD.29	Planning and progress reporting skills		X	
C.AUD.SD.30	Scope boundaries identification skills		X	
C.AUD.SD.31	Information gathering skills		X	X
C.AUD.SD.32	Evidence assessment and correlation skills		X	X
C.AUD.SD.33	Documentation review skills		X	X
C.AUD.SD.34	Observation skills		X	X
C.AUD.SD.35	Findings confirmation skills		X	X
C.AUD.SD.36	Samples NC extrapolation skills		X	X
C.AUD.SD.37	Conclusions building skills		X	X
C.AUD.SD.38	Evidence recording and audit trail generation skills		X	X
C.AUD.SD.39	Compiling audit results and audit report generation skills		X	
C.AUD.SD.40	Review and monitoring skills to:	X	X	

Required Competency		Audit Team Roles		
Reference	**Knowledge and Skills**	**Engagement Lead**	**Lead Auditor**	**Auditor**
	• Ensure compliance with all contractual and legal obligations including delivery of reports and recommendations to clients and stakeholders • Identify and address deviation from the agreed approach and plan to ensure delivery of agreed services with client • Ensure delivery of all outputs as per agreed quality and timelines • Assess the results and solve any unfinished items • Analyze audit results and ensure compliance to the reporting process			

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)

End of Document