الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

National Information Security Compliance Framework (NISCF) – Advisory Accreditation Requirements

[NCSA-NISCF-ACCR-ADV-RQT]

Requirements for Advisory Accreditation

National Cyber Security Agency (NCSA)

June 12, 2024

V1.3

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

Document Control

Document Details	
Document ID	NCSA-NISCF-ACCR-ADV-RQT
Version	V1.3
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 – Advisory Accreditation Requirements" - V1.3 - C0 – Public / PS1 – Non-Personal Data (Non-PD) in order to provide the requirements for applicants to NISCF's Advisory Accreditation Services, Accredited Service Providers, and for the delivery of Advisory related to NISCF's Services, as part of National Information Security Compliance Framework (NISCF) Accreditation 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 – Advisory Accreditation Requirements".

Any reproduction concerning this document with the intent of commercialization shall seek 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.

The assurance provided is not absolute and its based-on documents and information shared by the Service Providers and based on an assessment performed at a particular point in time. Therefore, NCSA does not hold responsibility of errors, damages or losses resulting from the usage of products or consumption of services provided by Accredited Service Providers.

LEGAL MANDATE(S)

Based on Emiri Decree No. 1 of the year 2021, the 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.

Advisory Accreditation Requirements

Domain	Control No.	Control Description
Requirement for Service Provider	**1.1**	**Legal and Contractual Matters**
	1.1.1	The Service Provider shall provide a valid company registration certificate, following applicable laws in the State of Qatar.
	1.1.2	The Service Provider shall provide its template of a legally enforceable agreement, that serves as a contract between the Service Provider and its clients for the provision of Advisory Services and that shall adhere to legal requirements in the State of Qatar.
	1.2	**Liability and Financing**
	1.2.1	The Service Provider shall provide evidence of annual insurance coverage (Professional Indemnity) covering least its Advisory Service offering. The Service Provider shall provide a written and approved justification of the coverage amount.
	1.2.2	The Service Provider shall provide the latest audited Financial Statements containing an unmodified opinion.
Structural Requirements	**2.1**	**Organizational Structure & Experience**
	2.1.1	The Service Provider shall provide a documented organizational structure with a clear identification of the department under which the Advisory Service operates and the related roles. The Service Provider shall also provide: • Documented evidence identifies the ultimate authority responsible for approving policies, processes, and procedures related to the Advisory Service's operation. • Total staff strength. • Key personnel and teams responsible for providing Advisory Services, including turnover and sub-contractor employees.
	2.1.2	The Service Provider shall demonstrate sufficient experience delivering Advisory Services, supported by a track record of successful engagements and expertise in relevant domains. To validate this experience, the Service Provider shall provide documentary evidence, including at least three references from clients where similar advisory services were undertaken within the last 3 years.
	2.2	**Control Environment**
	2.2.1	The Service Provider shall demonstrate commitment to integrity and ethical values.
	2.2.2	The Service Provider shall hold individuals accountable for their responsibilities when undertaking Advisory Services. The Service Provider shall ensure that it delivers the advisory service following the Code of Ethics and Professional Conduct (Appendix: Code of Ethics and Professional Conduct).
	2.2.3	The Service Provider shall maintain a documented service catalog outlining its Advisory Service offerings. Note: The catalog shall provide comprehensive information on the range of services including descriptions, scopes, and deliverables.

Domain	Control No.	Control Description
	2.2.4	The Service Provider shall have business continuity provisions and processes defined, that are regularly tested, and related to the Advisory Services.
Resource Requirements	**3.1**	**Competence of Management and Personnel**
	3.1.1	The Service Provider shall provide a process to ensure that personnel possess adequate knowledge relevant to the advisory activity, particularly within the information security and cybersecurity domain. Additionally: • The Service Provider shall define the competence necessary for each technical area and function. • The Service Provider shall establish methods for assessing and demonstrating competence before assigning personnel to specific functions.
	3.2	**Determination of Competence Criteria**
	3.2.1	The Service Provider shall maintain a documented process for establishing competence criteria for personnel engaged in Advisory Services, incorporating key aspects such as: • Determining competence criteria tailored to the requirements of each type of service delivery defined in the service catalog (please refer to requirement 2.2.3). • The output of this process shall consist of documented criteria delineating the necessary knowledge, skills, qualifications, and experience required for personnel to effectively perform their tasks and achieve desired outcomes.
	3.3	**Evaluation Processes**
	3.3.1	The Service Provider provides documented processes for both the initial assessment of competence and ongoing monitoring of competence and performance for all personnel engaged in the management and execution of Advisory Services, adhering to the determined competence criteria (as part of 3.2.1). Additionally, the Service Provider shall demonstrate the effectiveness of its evaluation methods.
	3.4	**Personnel Involved in the Advisory Services**
	3.4.1	The Service Provider shall demonstrate that Advisory Services leads possess the requisite knowledge, training, and certification for each type of service delivery defined in the service catalog (please refer to requirement 2.2.3). Note: This includes ensuring that leads are well-versed in relevant industry standards, regulations, best practices, and emerging trends within their respective domains.
	3.4.2	The Service Provider shall ensure the satisfactory performance of all personnel engaged in Advisory Services. Documented procedures and criteria shall be established for monitoring and measuring the performance of all individuals involved, considering the frequency of their involvement and the risk associated with their activities. Additionally, the Service Provider shall review the competence of its personnel based on their performance to identify any training needs.

Domain	Control No.	Control Description
	3.5	**Personnel Records**
	3.5.1	The Service Provider shall maintain up-to-date personnel records, including competence evidence documentation, and records of any relevant Advisory Services provided by each personnel.
	3.6	**Outsourcing**
	3.6.1	The Service Provider shall provide a documented policy and process delineating the conditions under which outsourcing activities may be undertaken. The document shall encompass criteria for selecting outsourcing partners, risk assessment procedures, contractual obligations, and mechanisms for monitoring and managing outsourced activities.
	3.6.2	The Service Provider shall have a standard legal agreement by which the outsourced personnel commits to comply with the Service Provider's applicable policies, processes, and procedures related to the Advisory Service activities. The agreement shall address confidentiality safeguards and mitigate conflict of interest.
Information Requirements	**4.1**	**Confidentiality and Publicity**
	4.1.1	The Service Provider shall provide evidence demonstrating the implementation of measures to safeguard confidential information. Additionally, the Service Provider shall ensure that all information disseminated to clients or the marketplace, including advertising materials, is accurate and devoid of misleading statements.
	4.1.2	The Service Provider shall have a legally enforceable agreement and implement policies to safeguard the confidentiality of information acquired or generated during the execution of Advisory Services across all levels of its organization, including committees, external entities, and individuals acting on its behalf.
	4.1.3	The Service Provider shall have policies and procedures to notify the client in advance of any information it intends to disclose in the public domain. All other information, excluding data made publicly accessible by the Client, shall be treated as confidential.
	4.1.4	The Service Provider shall provide policies and procedures to ensure adherence to Law No. 13, the Personal Data Privacy Protection Law (PDPPL), and applicable international regulations. Note: These policies shall delineate specific protocols governing the collection, utilization, retention, disclosure, and disposal of personal information and sensitive data.
	4.1.5	The Service Provider shall have policies and procedures to notify the National Cyber Security Agency (NCSA) in the event of any data breach or security incident. Note: This notification shall be made without undue delay upon discovery of the incident and shall include all pertinent details regarding the nature, scope, and impact of the breach or incident.
	4.1.6	The Service Provider shall have policies and procedures to uphold confidentiality and privacy data rights, ensuring that sensitive

Domain	Control No.	Control Description
		information is only shared with third parties in strict adherence to legal requirements or with explicit consent from the affected parties.
	4.1.7	The Service Provider shall provide policies, procedures, and agreements to ensure that personnel understand their obligations to protect sensitive information and refrain from unauthorized disclosure.
	4.1.8	The Service Provider shall have policies and procedures to ensure the availability and utilization of equipment and facilities that facilitate the secure handling of confidential information, including documents and records. Additionally, the Service Provider shall employ digital security measures such as encryption, access controls, and secure storage solutions to protect electronic records and data from unauthorized disclosure or tampering.
Process Requirements	**5.1**	**Advisory Service Delivery**
	5.1.1	The Service Provider shall demonstrate that its engagement leads, or project managers possess the necessary knowledge, skills, and competencies to proficiently manage projects in alignment with industry best practices and standards. Additionally, the personnel shall hold certification from an internationally recognized project management scheme.
	5.1.2	The Service Provider shall provide a structured project management approach for the delivery of their Advisory Services. This approach shall include clearly defined processes, methodologies, and tools to ensure effective planning, execution, monitoring, and control of projects. Key components of the project management approach shall encompass project initiation, scope definition, resource allocation, risk management, communication protocols, and stakeholder engagement strategies.
	5.1.3	The Service Provider shall document the Project Charter and establish a transparent process to demonstrate its engagement with the Client in comprehensively understanding project requirements, clarifying expectations, and collaboratively establishing the scope, objectives, and criteria for the advisory engagement
	5.1.4	The Service Provider shall have a valid National Information Assurance (NIA) Certification covering the Advisory Accreditation Service activities. Note: ISO 27001 valid Certification from a Certification Body recognized by the International Accreditation Forum (IAF) covering the scope, is acceptable if a commitment is provided to achieve NIA Certification within 3 years.
	5.1.5	The Service Provider shall have documented and approved information security policies and procedures covering: • Information Assets Management. • Confidentiality and Acceptable Use. • Identity and Access Management. • Incident Management. • Third-party Security Management; and • Physical Security.

Domain	Control No.	Control Description
	5.1.6	The Service Provider shall ensure regular assessment of all issues and risks throughout Advisory Services. This includes ongoing monitoring, evaluation, and mitigation of potential issues and risks that may impact the successful delivery of services or the achievement of project objectives.
	5.1.7	The Service Provider shall establish and maintain policies and procedures to prevent breaches of Intellectual Property (IP) requirements during the provision of Advisory Services. These policies and procedures shall outline guidelines for the identification, protection, and respectful use of intellectual property belonging to clients, third parties, or the Service Provider itself.
	5.1.8	The Service Provider shall provide a retention policy and records retention register that shall have a minimum retention of three (3) years of the records after completion of Advisory engagement.

Appendix: Code of Ethics and Professional Conduct

Principle	Description
Confidentiality	• Protect client privacy and information. • Abide by legal and contractual requirements. • Maintain confidentiality of client data. • Avoid unauthorized disclosure of information. • Obtain consent before sharing third-party information.
Integrity	• Acting with honesty and transparency in all communications. • Be truthful with clients, stakeholders, and others. • Disclose potential risks and dangers associated with activities.
Professionalism	• Upholding high ethical standards. • Maintain integrity and professionalism throughout engagements. • Respect intellectual property of others. • Report suspicious financial practices. • Continuously develop knowledge and skills. • Work only within your competence. • Respect colleagues by not using proprietary information or methodologies without permission.
Compliance	• Following relevant laws, regulations, and policies. • Adhere to established rules and instructions. • Be aware of and compliant with applicable laws and regulations related to assignments.
Management Consultancy Principles	• Delivering effective and ethical consulting services. • Avoid conflicts of interest and maintain objectivity. • Ensure advice considers client resources and practicality. • Prioritize client needs and objectives throughout the project lifecycle.
Additional Requirements	• Enhancing service delivery. • Define clear processes for project management (initiation, planning, execution, and closure). • Establish a framework for addressing potential conflicts. • Outline a commitment to continual improvement of services.
Respect	• Treating everyone with dignity and respect. • Treat all parties with respect, regardless of background, culture, or beliefs. • Avoid discrimination and harassment of any kind. • Recognize the importance of diversity and inclusion.

End of Document