الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

National Information Security Compliance Framework (NISCF) – General Taxonomy for National Accreditation

[NCSA-NISCF-ACCR-GTXD]

Document

National Cyber Security Agency (NCSA)

September 25, 2023

V1.0

Public

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Document Control

Document Details	
Document ID	NCSA-NISCF-ACCR- GTXD
External Version	V1.0
Classification & Type	Public
Abstract	This document is the General Taxonomy Document for National Accreditation developed by the National Cyber Security Agency (NCSA) with the intended usage in the operation of National Information Security Compliance Framework (NISCF) Accreditation Services. This document provides definition of key terminologies used in NISCF Accreditation Services.

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 (NISCF) – General Taxonomy for National Accreditation" - V1.0 - Public, in order to provide provides definition of key terminologies used in NISCF Accreditation Services.

NCSA is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge NCSA as the source and owner of the "National Information Security Compliance Framework (NISCF) – General Taxonomy for National Accreditation".

Any reproduction concerning this document with 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.

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 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

National Cyber Security Agency (NCSA) created its Accreditation Services to provide assurance that Service Providers have the capability and capacity to deliver cyber security related services in a specified subject or areas of expertise.

In effort to improve the Accreditation Services, NCSA developed this document, titled "National Information Security Compliance Framework (NISCF) – General Taxonomy for National Accreditation" - V1.0 - Public, to provide the cyber space with definition of key terminologies used in NISCF Accreditation Services.

2. Purpose and Scope

2.1. Purpose

The purpose of this document is to provide provides definition of key terminologies used in NISCF Accreditation Services.

2.2. Scope

The definition provided in the General Taxonomy Document for National Accreditation applies to all Accreditation Services that are offered by NCSA under the NISCF.

Definitions of terminologies can be provided in other documents of the NISCF, that may differ from these presented in this taxonomy document. In such cases, the definition provided in the other documents superspeed these ones defined in this document.

3. Key Definitions

Acceptance	The action of formally communicating to a Service Provider applying for NISCF's Accreditation Services that the request received is suitable.
Accreditation	Assurance that an entity has the capability and capacity to deliver cyber security related services in a specified subject or areas of expertise.
Accreditation Body	The moral entity that performs and provides NISCF Accreditation Services operation.
Accreditation Services	Services offered by the Accreditation Body that have for goal to provide Accreditation under the NISCF.
Accredited	Organization that has been granted an NISCF Accreditation Services Certificate of Accreditation.
Active	Not expired, withdrawn, suspended, or terminated Certificate of Accreditation.
Administrative safeguards	Establish standards and specifications for the NISCF Accreditation Services' Information Security Program.
Appeal	Request by an individual or an organization that is directly impacted by an NISCF Service decision made by NCSA to reconsider the decision that was made regarding its request for NISCF Service or its awarded certificate, title, credential or other demarcation
Applicant	The Service Provider that applied for NISCF Accreditation Services through formal request.
Area of expertise	A specific and particular field in Cyber Security.

Assessment	Process of getting a snapshot of the reality of a scope at a specific point in time to evaluate compliance. Assessment is similar to Audit, the difference is that Audit is more formal process, with higher level of assurance and more stringent evidence admissibility process.
Assurance	Reasonable level of confidence achieved by a third-party that an entity or an individual complies with and conforms to defined requirements, based on information provided by a trusted party.
Authoritative Power	The capability to use legitimacy to convince and govern.
Authorized Representative	A person chosen by the applicant to NISCF's Accreditation Services or Accredited Service Provider to act on its behalf in relation to NISCF's Accreditation.
Best practices	Commercial or professional procedures that are accepted or prescribed as being correct or most effective.
Black Box Testing	A testing methodology in which the penetration tester has no knowledge of the internal structure and implementation detail of the assessment subject.
Certificate of Accreditation	Document issued by the Accreditation Body to an Accredited Organization to evidence conformance to NISCF Accreditation requirements.
Complaint	Expression of dissatisfaction, other than appeal, by a third-party to NCSA relating to NISCF Services.
Compliance	The result of an entity meeting its obligations against a specified set of criteria.
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities or processes.

Conflict of interests	Situations that impair, or could reasonably be perceived by the National Cyber Security Ecosystem to impair, the objectivity of the Accreditation Body, persons in charge with its governance and / or management, employees, sub-contractors, and partners.
Conformance	Demonstrate that specific requirements are fulfilled.
Corrective Action Plan	A detailed plan of actions that is developed to achieve targeted outcomes for resolution of identified non-conformities.
Cyber Insurance	Cyber insurance is a risk treatment option that can compensate the insured against potentially significant financial losses associated with a cybersecurity incident. Cyber insurance is provided by an insurer who underwrites risks by signing and accepting liability, thus guaranteeing payment to the insured in case loss or damage occurs.
Decision	Conclusion, based on results of review, that fulfilment of specified requirements has or has not been demonstrated.
Demarcation	Actions leading to establishing boundaries or limits in relation to what is considered related or not to the NISCF Services.
Denial	Refusal of a request.
Eligible	Being suitable and having the right to perform a specific action or request specific service.
Employee	Person that has a direct employment contract with an entity.
Engagement	Formal agreement to perform defined operation.
Engagement Lead	The main individual that handles the engagement with the client.

Escalate privilege	A privilege escalation attack is a cyberattack designed to gain unauthorized privileged access to a system.
Evaluation	Combination of the selection and determination functions of conformance assessment operation.
Evidence	Information used by the Accreditation Body to conclude that a Service Provider is in conformance and compliance with a defined set of requirements or not.
Expiry	End of a period for which an element was considered valid.
Financial safeguards	Financial funds and controls to ensure going concern of and coverage of liabilities arising from the NISCF Accreditation Services.
Grey Box Testing	A hybrid testing methodology between black box and white box testing. In grey box testing, the internal structure is partially known.
Impartiality	Objectivity regarding the outcome of the Accreditation Body operation.
Intelligence Gathering	The process of collecting information on threats to people, buildings, or organizations with the purpose to be used during the testing and exploitation phases.
Legally enforceable agreement	Contract that holds its signatories legally accountable and / or responsible for the duties in defined the contract in a specified jurisdiction.
Maintenance	Iteration of conformance audits, assessments, evaluations, or examinations operation basis for maintaining the validity of a Certificate of Accreditation.
Mutually Exclusive	Two or more events that cannot happen simultaneously.

National Cyber Security Agency	The Agency that unifies the visions and efforts of securing the State of Qatar cyberspace and maintaining national cyber security.
National Information Assurance Framework	The registry of cyber security laws, policies, standards, and guidelines, owned by the National Cyber Security Agency (NCSA).
National Information Security Compliance Framework	The umbrella under which all compliance initiatives, owned by the National Cyber Security Agency (NCSA) or other government or non-government entities, directly or indirectly, that have for primary goal to provide cyber security assurance and can have a material impact on national Qatar cyber security ecosystem, are developed and maintained.
NISCF's Accreditation Services Agreement	Legally enforceable agreement signed between the applicant and the Accreditation Body to govern the relationship related to a NISCF's Accreditation Services request.
Normative	Aspects of a standard that shall be strictly followed, implemented, and conformed to, in order to be comply with the standard.
Operation	Activities performed by the Accreditation Body and / or third-parties on behalf of the Accreditation Body to be able to make a decision related to NISCF Accreditation Services.
Organization Structure	Outlines the way activities are directed by specific components of the organization to achieve the goals of an organization.
Outsourcing	Agreements with any other legal entity, other than the Service Provider applying for NISCF's Accreditation Service for providing resources on a punctual or continuous basis.
Partner	Organization that has contractual relationship with the Accreditation Body in relation to NISCF Accreditation Services.

Penetration Tester	Individual performing the Penetration Test activity.
Penetration Testing Accreditation Service	A form of ethical cybersecurity assessment to improve the risk posture which involves in-depth & majorly manual assessment tests in a defined scope to identify and exploit vulnerabilities affecting IT resources to mitigate or minimize the risk of malicious exploitation or attacks.
Period of validity	The period for which a Certificate of Accreditation is valid since its issuance until the next Re-Accreditation subject to successful maintenance.
Persons in charge with Governance and / or Management	The person(s) or organization(s) with the responsibility for the governance and management activities of an entity.
Police Clearance Certificate	A police clearance certificate is an official document issued as a result of a background check by the police or government agency of a country to enumerate any criminal records that an individual may have.
Policy	A formal statement of a principle (an organizational decision) that should be followed by its intended audience to achieve the stated objectives of the organization.
Procedure	Defines the established and / or mandatory way of performing the steps or actions defined in a process.
Process	Defines the series of steps or actions (including the inputs, outputs, and processing) that needs to be taken in order to achieve a particular objective.
Professional Indemnity Insurance	Insurance coverage to protect against a wide range of risks and can help the Service Provider to manage its financial and legal obligations in the event of a liability issue.

Re-Accreditation	Extension of the period of validity of a Certificate of Accreditation for an additional period of validity.
Record	Physical or logical to keep information as evidence.
Regulation	Set of rules published by an authorized government entity that has the authority to act as a regulator for a sector or topic.
Reinstatement	Restoration of the full or partial restriction made during suspension on a Certificate of Accreditation.
Rejection	The action of formally communicating to an applicant that the request received is not suitable.
Request	Formal written demand made by the applicant and / or other stakeholders related to a NISCF's Accreditation Services request through specified means toward the Accreditation Body and / or a third-party acting on its behalf.
Responsibility	Duty to perform actions as intended by the owner.
Risk	The effect of uncertainty on objectives
Risk Management System	A system of coordinated activities to direct and control an organization with regard to risk.
Rules of Engagement (RoE)	Describes the target systems, scope, constraints, and proper notifications and disclosures of the Penetration Testing Service
Safeguards	Actions, individually or in combination, that are taking by the Accreditation Body 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 Accreditation Body.

Scope	The service types and delivery models of a specific NISCF Accreditation Service request or a NISCF Certificate of Accreditation.
Scope expansion	Expanding the scope of a Certificate of Accreditation after its issuance and while being active (Not expired, withdrawn, suspended, or terminated).
Scope reduction	Reducing the scope of a Certificate of Accreditation after its issuance and while being active (Not expired, withdrawn, suspended, or terminated).
Service Provider	An organization that provides a cyber security related service that is the core of the NISCF's Accreditation Service to third parties.
Service Provider's Team	The team that is solely composed of personnel that take part in the delivery of the Accreditation Service and have a direct legal agreement (employment or service contract) with the Service Provider.
Standard	Defines the requirements that needs to be met in application of policies.
Sub-contracting	The practice of assigning, part or all of the obligations and responsibilities under a contract with a client, to a third-party (organization or individual), as an undertaking.
Suspension	Temporary restriction on a Certificate of Accreditation for all or part of the scope.
Symbol	Mark, character, or graphical design used to represent a NISCF Service.
Technical safeguards	Hardware, software, and other technology-oriented means that limits access to NISCF Accreditation Services' Information.

Termination	Stoppage of the validity of the Certificate of Accreditation definitely, based on the Accredited Service Provider request.
Threat Agents	An individual or group that acts, or has the power to, exploit a vulnerability or conduct other damaging activities
Threat Modeling	A process to identify and enumerate potential threats such as vulnerabilities or lack of defense mechanisms and prioritize security mitigations
Title	Denomination used to identify a person, an organization, group of persons or organizations in relation to the NISCF Services.
Transition	The process of changing from one state to another.
Unscheduled Assessment	An assessment during the NISCF's Accreditation Services lifecycle that is not the initial assessment, Maintenance or Re-Accreditation.
Valid	Something that is genuine and considered as authentic and accepted.
Vetting	The process of performing a background check on someone before offering them employment, conferring an award, or doing fact-checking prior to making any decision
Vulnerability Analysis	A systematic review of security weaknesses in an information system
White Box Testing	A testing methodology in which the penetration tester has extensive knowledge of the internal structure and implementation detail of the assessment subject.
Withdrawal	Revocation of Certificate of Accreditation by the Accreditation Body.

End of Document