الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

National Information Security Compliance Framework (NISCF) – Accreditation Penetration Testing Standard

[NCSA-NISCF-ACCR-PNT-STND]

Requirements for Accreditation of Penetration Testing Service Providers

National Cyber Security Agency (NCSA)

February 8, 2024

V1.1

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

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Document Control

Document Details	
Document ID	NCSA-NISCF-ACCR-PNT-STND
Version	V1.1
Classification and 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 (NISCF) – Accreditation Penetration Testing Standard" - V1.1 - C0 – Public / PS1 – Non-Personal Data (Non-PD) in order to provide the requirements for applicants to NISCF's Penetration Testing Accreditation Services, Accredited Penetration Testing Service Providers and for the delivery of Penetration Tests related to NISCF's 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 – Penetration Testing 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.

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.

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 Penetration Testing Service Accreditation for Service Providers that offer Penetration Testing for their clients and are interested in showing to their clients, potential clients and other stakeholders that they demonstrated conformance with best practices related to the delivery of Penetration Testing services.

Service Providers shall comply with the requirements defined in this standard for the purpose of obtaining Accreditation and ongoing maintenance.

Penetration Testing Accreditation scope excludes following activities: Industrial Control Systems (ICS) or Operational technology (OT) Testing, Automated Vulnerability Assessment Scans, Threat Intelligence/Detection/Hunting, Crowd sourced Testing (Bug Bounty), Source Code Audit, Incident Response and Security Operations Center (SOC).

2. Purpose and Scope

2.1. Purpose

The purpose of this document is to provide requirements for Service Providers willing to request for NISCF's Penetration Testing Accreditation Service, Accredited Penetration Testing Service Providers and for the delivery of Penetration Tests related to NISCF's Services.

2.2. Scope

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

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

Penetration Testing Accreditation scope excludes following activities: Industrial Control Systems (ICS) or Operational technology (OT) Testing, Automated Vulnerability Assessment Scans, Threat Intelligence/Detection/Hunting, Crowd sourced Testing (Bug Bounty), Source Code Audit, Incident Response and Security Operations Center (SOC).

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).

4. Standard Requirements

G. Governance

G.1. Organizational Environment, Monitoring, Quality and Review

G.1.1. Legal Entity

G.1.1.1. The Service Provider shall provide a valid company registration certificate, in accordance with applicable laws in the State of Qatar.

G.1.2. Audited Financial Statements

G.1.2.1. The Service Provider shall provide the latest audited Financial Statements that shall contain an unmodified opinion.

G.1.3. Liability and Insurance

G.1.3.1. The Service Provider shall provide evidence of annual insurance coverage (Professional Indemnity and Cyber Insurance) covering least its Penetration Testing Service offering. The Service Provider shall provide a written and approved justification of the coverage amount.

G.1.4. Organizational Structure with, Duties, Responsibilities, and Authorities of Management

G.1.4.1. The Service Provider shall provide a documented organizational structure with clear identification of the department under which the Penetration Testing Service is operating and the related roles.

G.1.4.2. The Service Provider shall provide documented job descriptions of the different roles in the Service Provider's Penetration Testing Team.

G.1.4.3. The Service Provider shall provide documented evidence clearly identifying the person, unit or committee having the ultimate authority for the approval of policies, processes, procedures, methodologies related to the operation of the Penetration Testing Service.

G.2. Principles, Policies and Processes

G.2.1. Personnel Management Process

G.2.1.1. The Service Provider shall provide its Personnel Management Process that shall include:

- A process for hiring personnel, as part of the Service Provider's Penetration Testing Team, that shall include a competencies assessment step; and
- A process for on-going competencies monitoring of personnel involved in the delivery of the Penetration Testing Service, at least once in every calendar year (Annually), based on competencies criteria.

G.2.2. Outsourcing

G.2.2.1. The Service Provider shall provide a documented outsourcing process of personnel as a part of the Service Provider's Penetration Testing Team that shall cover or refer to:

- The risk management to identify, evaluate, mitigate and monitor risks associated with procuring outsourced Penetration Testers;
- The vetting of the outsourced personnel in conformance with the process provided in reference to requirement **G.3.3.1**; and
- The competencies evaluation of the outsourced personnel in conformance with requirement **G.3.1.1**.

NOTE: Interfirm outsourcing or the use of an individual or employee of another legal entity, individually contracted or otherwise, to take part in the delivery of the Penetration Testing Service, does constitute outsourcing. If the Service Provider does not use third parties, the Service Provider shall provide evidence in form of an approved written policy or official communication from an authorized person formally stating the prohibition of outsourcing.

G.2.2.2. The Service Provider shall have a standard legal agreement by which the outsourced personnel commit to comply with the Service Provider's applicable policies, processes, and procedures related to the Penetration Testing Service activities. The agreement shall address confidentiality safeguards and compliance with personal data protection requirements, in accordance with State of Qatar Laws and Regulations.

NOTE: In cases where a policy document is used to outline the above obligations, the agreement shall reference and acknowledge the provisions stated in the policy and the policy shall be provided.

G.3. People, Skills, and Competencies

G.3.1. Personnel Record, Evaluation and Code of Ethics

G.3.1.1. The Service Provider shall provide the Personnel Record Form for all personnel in the Service Provider's Penetration Testing Team (including outsourced personnel) that:

- Constitutes the exhaustivity of the Service Provider's Penetration Testing Team and will be the only reference in the Accreditation as of the allowed personnel to participate in Penetration Testing engagements;
- Evidences competency evaluation (against the defined in section **6.2. Service Provider's Penetration Testing Team Competencies Requirements**); and
- Documents the personnel commitment to the **Code of Ethics and Professional conduct**.

Note: Post-Accreditation the Personnel Record Form shall be updated annually as part of the on-going competencies monitoring (please refer to requirement **G.2.1.1**) and recorded for new personnel enrolled in the Service Provider's Penetration Testing Team (please refer to requirement **G.2.1.1**) and submitted during each Maintenance.

G.3.2. Knowledge Management

G.3.2.1. The Service Provider shall provide an annual training plan for all the personnel of the Service Provider's Penetration Testing Team.

Note: The trainings selection shall be justified through needs or gaps in competencies (please refer to requirement **G.3.1.1**) following the Service Provider needs, ongoing monitoring of competencies.

G.3.3. Personnel Requirements

G.3.3.1. The Service Provider shall provide a documented process for vetting of the Service Provider's Penetration Testing Team, and the supporting evidence that is has been applied for all personnel, that shall include at least:

- Verification of employment history and qualifications;
- Background checks with the objective of identifying illegal or unethical online activities; and
- Past criminal convictions.

G.3.3.2. The Service Provider shall maintain as part of the Service Provider's Penetration Testing Team at all times:

- At minimum one (1) Engagement Lead[1]; and
- At minimum one (1) Penetration Tester for each type of Penetration Testing (please refer to requirement **S.1.1 Service Types**) selected as Accreditation scope.

  Note: The same personnel can fulfil the role of Penetration Tester for more than one type of Penetration Testing selected as Accreditation scope, under the conditions that, he/she evidences competencies required, based on the competency evaluation performed (please refer to requirement **G.3.1.1**) for the each type of Penetration Testing he/she is appointed to perform.

[1] In accordance with the NISCF Accreditation Terms and Conditions, the Engagement Lead shall not be outsourced.

M. Management

M.1. Security and Risk Management

M.1.1. Compliance and Security Requirements

M.1.1.1. The Service Provider shall have documented and approved information security policies and procedures[2] covering:

- Information Assets Management;
- Confidentiality and Acceptable Use;
- Identity and Access Management;
- Incident Management;
- Third-party Security Management; and
- Physical Security.

M.1.1.2. The Service Provider shall have a valid National Information Assurance (NIA) Certification covering the Penetration Testing Accreditation Service activities.

Note: ISO 27001 valid Certification from a Certification Body recognized by International Accreditation Forum (IAF) covering the scope, is acceptable, if a commitment is provided to achieve NIA Certification within 3 years.

M.1.1.3. The Service Provider shall retain and archive in a secure, encrypted and redacted format all scans, tests, exploitations performed, additional post-exploitation, reporting and corresponding evidence of a Penetration Testing engagement.

M.1.1.4. 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 referred to in requirement **M.1.1.3** after completion of a Penetration Testing engagement.

M.1.1.5. The Service Provider shall have a documented secure cleaning and removal process of the tools, credentials and accounts added to the scope during a Penetration Testing engagement.

[2] National Information Assurance (NIA) Standard can be used as reference to develop the required policies and procedures.

M.1.2. Tools and Systems

M.1.2.1. The Service Provider shall provide detailed information about the tools used during Penetration Testing engagements, including the tool name, description, intended usage, and an assessment of associated risks.

M.1.2.2. The Service Provider shall provide evidence of segregated testing machines for Penetration Testing engagements, ensuring that each machine undergoes sanitization upon completion of its respective engagement.

M.1.2.3. The Service Provider shall establish and maintain a segregated or isolated environment dedicated solely to Penetration Testing activities.

Note: This environment, inclusive of testing machines, hardware, networks, and software, shall be separate from the Service Provider's corporate infrastructure.

S. Service (Penetration Testing)

S.1. Catalogue

S.1.1. Service Types

S.1.1.1. The Service Provider shall select during its application to NISCF's Penetration Testing Accreditation Service the Penetration Testing Service types it offers, that are wanted to be included in the scope of its Accreditation:

- **Internal Penetration Testing:** A Penetration Testing conducted from within an organization's network to identify vulnerabilities and security weaknesses that could be exploited by an insider or an attacker who has breached the external defenses. This form of testing assesses the strength of internal security controls, the potential for lateral movement, and the ability to access sensitive information or critical systems.
- **External Penetration Testing:** A Penetration Testing aimed at identifying and exploiting vulnerabilities in an organization's external-facing systems, such as websites, email servers, and firewalls, from the perspective of an external attacker. It evaluates the security of an organization's perimeter defenses and the effectiveness of its detection and response mechanisms.
- **Red Teaming:** A comprehensive and multi-layered attack simulation aimed at assessing the effectiveness of an organization's security posture. It employs strategies and techniques used by real-world attackers, including social engineering, physical security breaches, and advanced persistent threats, to identify vulnerabilities across people, processes, and technology.

S.1.2. Service Delivery Models

S.1.2.1. The Service Provider shall select during its application to NISCF's Penetration Testing Accreditation Service the Penetration Testing Service delivery models it offers, that are wanted to be included in the scope of its Accreditation:

- **On-site testing model**: A Penetration Testing that is performed from the client's location and premises.
- **Remote testing model**: A Penetration Testing that is performed outside of the client's location and premises.

S.1.3. Service Provider's Penetration Testing Catalogue

S.1.3.1. The Service Provider shall provide a documented service catalogue detailing its Penetration Testing Services offering.

S.1.3.2. The Service Provider shall provide detailed capability statements for each of the Penetration Testing Services detailed in its Service Catalogue shared in response to requirement **S.1.3.1**, and provide a detailed mapping of these Services to the Service Types selected in **S.1.1.1** and Delivery Models selected in **S.1.2.1**.

S.2. Methodologies

S.2.1. Penetration Testing Methodologies

S.2.1.1. The Service Provider shall have a documented and approved Penetration Testing methodologies for each type of the Penetration Testing Service selected (see section **S.1.1 Service Types**) that details and cover all the requirements defined under the sections **S.3.1. Engagement**, **S.3.2. Planning and Scoping**, **S.3.3. Exploitation Exercise**, **S.3.4. Post Exploitation Activity** and **S.3.5. Reporting**, and all their related requirements, and shall keep documented records of conformance of each Penetration Testing engagement performed with the methodologies.

Note: The methodologies shall be based on best practices (e.g., Open Source Security Testing Methodology Manual (OSSTM), SP800-115 (3), Open Web Application Security Project (OWASP), Information Systems Security Assessment Framework (ISSAF), Penetration Testing Execution Standard (PTES)…) and /or National Standards and Guidelines issued by the National Cyber Security Agency (NCSA) or other sectorial authorities within the State of Qatar.

S.3. Delivery

S.3.1. Engagement

S.3.1.1. The Service Provider shall have a Non-Disclosure Agreement (NDA) template that shall be signed with the client before gaining access to any information related to a Penetration Testing engagement.

S.3.1.2. The Service Provider shall provide and use its standard legally enforceable agreement document for providing Penetration Testing Service that serves as a contract between the Service Provider and its client that shall include the following elements:

- Scope of services: A clear description of the Services being provided, including any specific tasks or deliverables;

- 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);
- Indemnification: A provision stating the conditions under which the Service Provider will indemnify its client against claims or damages resulting from the services provided;
- Liabilities: The liabilities limitations of the Penetration Testing for the Service Provider;
- Information sharing: A provision stating that the Service Provider may share specific non-sensitive information related to Penetration Testing engagements with the National Cyber Security Agency (NCSA) in its capacity of the regulatory authority for Cyber Security domain; and
- Terms and conditions: The terms and conditions under which the services will be provided.

S.3.2. Planning and Scoping

S.3.2.1. The Service Provider shall collect from the client the different business and cyber risks associated with the Penetration Testing engagement (e.g., Business Impact Assessment, Data Protection Impact Assessment...).

S.3.2.2. The Service Provider shall have applicable laws and regulations registry related to sectors for which it provides Penetration Testing Services, inform the client of them.

S.3.2.3. The Service Provider shall have a documented risk register with risk scenarios based on the **Service Types**, **Service Delivery Models** and Penetration Testing styles (i.e., Black box, Grey Box or White Box) and shall document the communication of such risks to the client and ensure the later understands and accept those risks.

S.3.2.4. The Service Provider shall have a documented planning and scoping templates that shall be followed and documented in Penetration Testing engagements, which include at least the following:

- A brief description of the approach, constraints, and the planned attack techniques, tactics and procedures;
- The Penetration Testing time frame for exploitation;

- Single Point of Contact (SPOC) and Technical points of contact (TPOC);
- The selected engagements team members and their assigned roles; and
- The Penetration Testing Rules of Engagement (RoE) covering at least:
    I. Scope and limits of the tests;
    II. The reporting method of changes introduced to the scope during the engagement by the Penetration Tester; and
    III. Reference to the secure cleaning and removal process to be followed, after the completion of the engagement.

S.3.2.5. The Service Provider shall collect explicit documented authorization from the client before starting any exploitation activities, authorizing the activities in accordance with the communicated RoE and the Penetration Testing schedules.

S.3.3. Exploitation Exercise

S.3.3.1. The Service Provider shall establish and maintain a documented Intelligence Gathering Plan.

Note: Intelligence Gathering shall be performed unless specifically excluded by the client as per legally enforceable agreement or RoE.

S.3.3.2. The Service Provider shall conduct and maintain a documented Threat Modeling Plan for Penetration Testing engagement.

Note: Threat Modeling shall be performed unless specifically excluded by the client as per legally enforceable agreement or RoE.

S.3.3.3. The Service Provider shall establish and maintain a comprehensive Vulnerability Analysis Plan for each Penetration Testing engagement that shall encompass the following key components:

- Methods and tools involved in the identification of detected vulnerabilities;
- Confirmation of the vulnerabilities (e.g., elimination of false positives…); and
- Research on the confirmed vulnerabilities for further exploitation.

S.3.3.4. The Service Provider shall have documented and standardized exploitation checklists of techniques, tactics and procedures considering international best practices and /or National Standards and Guidelines issued by NCSA (e.g., OWASP Web Application Penetration Checklist, MITRE ATT&CK

Techniques, ...) to be used and tailored during a in Penetration Testing engagement.

S.3.4. Post Exploitation Activity

S.3.4.1. The Service Provider shall document Post Exploitation activities, if agreed with the client, considering the following:

- Restricted information and systems that Penetration Testers shall not access and prohibited activities (e.g., Any usage of super admin, any kind of dumping / collecting for tier 0 information / credentials considered a post exploitation…);
- Analysis of the compromised targets;
- Rediscovery based on the compromised targets; and
- Escalation of privileges.

S.3.4.2. The Service Provider shall apply and document systematically the application of the secure cleaning and removal process (please refer to requirement **M.1.1.5**) to ensure the complete eradication of any artifacts introduced during the testing and to maintain the security and integrity of the client's systems.

S.3.5. Reporting

S.3.5.1. The Service Provider shall provide a Penetration Testing Report (PTR) standard template for reporting, which shall be used to report on each Penetration Testing engagement, that shall include at least the following:

- Executive Summary that shall include:
  I. The Penetration Testing Objective;
  II. Presentation of the overall posture;
  III. General findings;
  IV. Recommendation summary;
  V. Issues, restrictions, or limitations encountered during the Penetration Testing engagement.
  VI. Duration of the Penetration Testing Engagement: The duration should cover the time from the initiation of testing activities to the conclusion of the post-exploitation phase.

- Detailed Report that shall include:
    I. Scope;
    II. The different types of tests performed and the tools used;
    III. Technical Findings Summary / Ranking / Methodology / Proof of Concepts (POC);
    IV. Vulnerability Rating, based on public information databases - CVEs, CWEs, OWASPs;
    V. Reasonable level of recommendation and guidance to the client to remediate the findings; and
    VI. Evidence of clean up post engagements and additional related Observations, Recommendations and Guidance.

S.3.5.2. In case of a retest is performed, the PTR shall specify if the test was a complete retest or if it was limited to a validation of previous findings. Follow-up PTR limited to previous findings validation shall include the disclaimer that the follow-up PTR may invalidated previous findings and shall not be regarded as the final and sole PTR for the engagement.

S.3.5.3. The PTR shall be signed by an authorized person, who could legally engage the responsibility of the Service Provider.

S.3.5.4. The Service Provider shall organize a closure meeting to discuss and explain the findings and obtain documented approval from the client for the PTR and any relevant agreements as the closure of the Penetration Testing engagement.

S.3.5.5. The Service Provider shall provide, as part of the request for NISCF's Penetration Testing Accreditation, at least three (3) examples of normalized Penetration Testing reports provided for previous Penetration Testing engagements for each of the Penetration Testing Service Type selected (see section **S.1.1. Service Types**) including at least the following items:

- Scope of testing;
- Methodology used;
- Summary of findings; and
- Severity of the vulnerabilities identified.

S.3.5.6. The Service Provider shall also provide the reference letters and / or delivery acceptance letters from the clients, demonstrating the delivery of the service and the achievement of the outcome, for the normalized Penetration Testing reports shared in response to requirement **S.3.5.5**.

5. Compliance and Enforcement

5.1. Compliance Process

All applicants to NISCF's Penetration Testing Accreditation Services and Accredited Penetration Testing 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 February 10, 2024.

5.3.2. Transition period

Not Applicable.

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 Penetration Testing Accreditation Services and Accredited Penetration Testing 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

CVE	Common Vulnerabilities and Exposures.
CWE	Common Weakness Enumeration.
NCGAA	National Cyber Governance and Assurance Affairs.
NCSA	National Cyber Security Agency.
NDA	Non-Disclosure Agreement.
NIA	National Information Assurance.
NISCF	National Information Security Compliance Framework.
PTR	Penetration Testing Report.
POC	Proof of Concept.
RoE	Rules of Engagement.
SPOC	Single Point of Contact.
TPOC	Technical Point of Contact.

6.2. Service Provider's Penetration Testing Accreditation Team Competencies Requirements

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

Required Competencies		**Penetration Testing Accreditation Service Team Roles**	
Reference	**Knowledge and Skills**	**Lead Engagement Role**	**Penetration Testers Role**
General			
Knowledge Statements			
K.PNT.G.1	Knowledge of capability and capacity management	X	
K.PNT.G.2	Knowledge of risk assessment and management methodologies	X	
K.PNT.G.3	Knowledge of information security controls and their objectives	X	X
K.PNT.G.4	Knowledge of confidentiality protection best practices	X	X
Practical Skills Statements			
PS.PNT.G.1	Project management skills	X	
PS.PNT.G.2	Communication and leadership skills	X	
PS.PNT.G.3	Resources and team management skills	X	
PS.PNT.G.4	Problem management skills	X	
PS.PNT.G.5	Negotiation skills	X	
PS.PNT.G.6	Presentation skills	X	X
PS.PNT.G.7	Finding summarizing and drafting skills		X
PS.PNT.G.8	Reporting skills	X	X
Service Delivery: Penetration Testing Service			
Knowledge Statements			
K.PNT.SD.1	Knowledge of Penetration Testing principles	X	X
K.PNT.SD.2	Knowledge of the industry standards and regulations related to Penetration Testing, including Ethics and Code of Conduct	X	X
K.PNT.SD.3	Knowledge of legal and contractual tools to authorize Penetration Testing	X	X
K.PNT.SD.4	Knowledge of Penetration Testing methodologies based on Penetration Testing types and delivery models	X	X

Required Competencies		Penetration Testing Accreditation Service Team Roles	
Reference	**Knowledge and Skills**	**Lead Engagement Role**	**Penetration Testers Role**
K.PNT.SD.5	Knowledge of Penetration Testing engagement key stakeholders and their roles and responsibilities	X	X
K.PNT.SD.6	Knowledge of common operating systems and networking protocols		X
K.PNT.SD.7	Knowledge of common vulnerabilities		
K.PNT.SD.8	Knowledge of attack tactics, techniques and procedures		X
K.PNT.SD.9	Knowledge of vulnerability analysis and exploitation automated tool suites		X
K.PNT.SD.10	Knowledge of engagement closure practices	X	
Practical Skills Statements			
PS.PNT.SD.1	Engagement risk management skills	X	
PS.PNT.SD.2	Penetration Testing scoping skills, including the selection of the adequate approach and controls	X	X
PS.PNT.SD.3	Planning and progress reporting skills		X
PS.PNT.SD.4	Scope boundaries identification skills		X
PS.PNT.SD.5	Information gathering skills		X
PS.PNT.SD.6	Threat Modeling and vulnerability assessment skills		X
PS.PNT.SD.7	Exploitation skills based on Penetration Testing types		X
PS.PNT.SD.8	Information Security Testing Tools skills		X
PS.PNT.SD.9	Code and scripts creation and customization skills		X
PS.PNT.SD.10	Malicious software usage skills		X
PS.PNT.SD.11	Privileges escalation skills		X
PS.PNT.SD.12	Evidence recording and audit trail generation skills		X
PS.PNT.SD.13	Compiling Penetration Testing results and Penetration Testing Report (PTR) generation skills		X
PS.PNT.SD.14	Review and monitoring skills of Penetration Testing engagement and Penetration Testers activities.	X	

6.3. Code of Ethics and Professional Conduct

- Abide by legal, regulatory and contractual confidentiality requirements.
- Integrity is maintained at all time that translates in honesty and transparency in all communications with clients, stakeholders, and other parties.
- Maintain confidentiality and protecting the privacy of clients and their data.
- Never disclose any confidential information about the client to any person, including the organization employees who are unauthorized to access or do not need such information.
- Take precautionary measures to avoid unauthorized disclosure of confidential information.
- Any third-party information shall be only shared with prior consent from all stakeholders.
- Always ensure full disclosure of risks and potential dangers of the Penetration Testing activities to all stakeholders involved.
- Maintain professionalism at all times and commit to skills and competencies improvement.
- Always use software or process that is obtained legally and ethically.
- Always protect the intellectual property of others.
- Shall not engage in deceptive or improper financial practices and shall report any suspicion to the competent authorities.
- Shall always respect the scope boundaries of the engagement and shall log any violations committed.
- Ensure all Penetration Testing activities are authorized by all stakeholders and within legal limits.
- Proper authorization and consent need to be obtained for the use of the client/ employer system and property.
- Shall 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.

- Shall not make inappropriate reference to the NCSA's Accreditation or Certification or misleading use of certificates, marks or logos in publications, catalogues, documents, or talks.
- Shall always adhere to rules, regulations, instructions, and policies and shall not have convict in any felony or violate any law.
- Uphold the reputation of the cybersecurity industry by adhering to recognized standards and best practices.
- Continuously improve your knowledge and skills through training and professional development. Always perform work only in areas of your competence.
- Strive to provide high-quality and accurate reports, detailing penetration testing findings, recommendations, and remediation measures.
- Treating all parties with dignity and respect, regardless of their background, culture, or beliefs.
- Respecting the confidentiality and privacy of clients and their data.
- Avoiding discrimination or harassment of any kind.
- Recognizing the importance of diversity and inclusion in the cybersecurity industry.

6.4. Reference

Emiri Decree No 1 of year 2021.

President of National Cyber Security Agency (NCSA) Decision No 3 of year 2022.

NCSA-NISCF-ACCR-GTXD (General Taxonomy Document for National Accreditation - Public).

NCSA-NISCF-ACCR-GPNA (General Policy for National Accreditation - Public).

NCSA-NISCF-ACCR-SNA (Standard for National Accreditation - Public).

NCSA-NISCF-ACCR-POSS (Accreditation Processes - Public).

ISO/IEC 31000:2018 https://www.iso.org/standard/65694.html

PTES (Penetration Testing Execution Standard): This is a comprehensive framework for conducting penetration tests, covering everything from planning to reporting. https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf

PCI QSA Penetration Testing Guidance: This information supplement provides general guidance and guidelines for penetration testing.
https://listings.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

FedRAMP Requirements and Penetration Test Guidance
https://a2la.qualtraxcloud.com/ShowDocument.aspx?ID=5621
https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf

US GSA IT – Conducting Pentest Exercises
https://www.gsa.gov/cdnstatic/Conducting-Penetration-Test-Exercises-[CIO-IT-Security-11-51-Rev-6]-11-25-2022.pdf

End of Document