National Cyber Emergency Response Team

Criteria for Information Security Consultant Registration

Scope

Registration criteria of information security professionals for engagement in providing Pakistan Information Security Framework (PISF) implementation consultancy and audit readiness support services with expertise in three different domains: IT, OT and Cloud.

Description

This criterion pertains to registration from qualified information security professionals for engagement in providing Pakistan Information Security Framework (PISF) implementation consultancy and audit readiness support services with expertise in three different domains: IT, OT and Cloud.

The purpose of this initiative is to assist organizations in strengthening their information security posture, achieving compliance with prescribed security requirements, and preparing effectively for formal assessments and audits. Selected consultants will be responsible for conducting gap assessments, developing implementation roadmaps, providing technical and governance guidance, supporting control implementation, and facilitating audit readiness activities in accordance with applicable regulatory and security standards.

General Consultant Levels

The consultant roles are divided into three categories based on experience, qualifications, certifications, and practical expertise:

- Expert Consultant
- Senior Consultant
- Junior Consultant

Following are the domains of expertise where applicants can apply for security consultancy:

- IT
- Cloud
- OT

Category Classification

Category	Organization Type	Scope
CAT-I	Critical Sectors	Highest security requirements IT/OT/Cloud security (More than 150 nodes)
CAT-II	Critical Sectors	Enhanced security IT/OT/Cloud security (Up to 150 nodes)
CAT-III	Non-Critical Sectors	Intermediate security IT only (More than 150 nodes)

Category	Organization Type	Scope
CAT-IV	Non-Critical Sectors	Baseline security IT Services only (Up to 150 nodes)

Note: *All sectors/organizations designated as Critical shall fall into CAT-I and CAT-II categories, while those not included in Critical shall be categorized as CAT-III and CAT-IV*

Consultant Deployment Based on Organization Category

To ensure appropriate expertise and risk-based engagement, consultant deployment shall be aligned with the category of the organization being assessed.

Category I & II Organizations

For Category I & II organizations, only an Expert Consultant will be engaged to lead and perform the cyber security assessment, implementation consultancy and audit readiness. This requirement is intended to ensure that highly critical organizations are assessed by consultants with the highest level of experience, qualifications, and domain expertise.

Expert consultant may also be assisted by Junior consultant wherever required by the organization.

Category III & IV Organizations

For Category III & IV organizations, a Senior Consultant or Expert Consultant may be engaged to carry out the required cyber security assessment and related activities. The Senior Consultant must meet all prescribed eligibility criteria and possess sufficient experience to handle medium-to-high complexity environments.

Expert/ senior consultant may also be assisted by Junior consultant wherever required by the organization.

Vulnerability Assessment & Penetration Testing Services

Junior Consultants may also be independently engaged to conduct vulnerability assessments, and penetration testing activities in Category III or IV organizations. These consultants must fulfil the required minimum qualifications, technical certifications, and practical experience criteria as defined in this document.

Expert Consultant Criteria

Educational and Experience Requirements

An Expert Consultant must:

Hold a bachelor's degree in Computer Science, Information Technology, Cyber Security, Information Security, or an equivalent field and possess at least 12 years of total IT and information security experience. Out of this, a minimum of 6 years should specifically be in cyber security and at least 3 years

must involve experience in fields like GRC, Risk assessments, security/ compliance audits, vulnerability assessments/penetration testing.

Or

Hold MS/ PhD in Information/ Cyber Security or related field and possess at least 8 years of total IT and information security experience. Out of this, a minimum of 5 years should specifically be in cyber security and at least 3 years must involve experience in fields like GRC, Risk assessments, security/ compliance audits, vulnerability assessments/penetration testing.

And

Must Possess an experience of at least 10 Audits or Compliance preparedness engagement, gap assessments, risk assessments.

Core Certifications

The consultant must hold at least two certifications, one Certifications like: CISSP, CISM, CRISC, CISA, ISO 27001 LA/ LI or equivalent

And one certification based on domain expertise:

For IT: CISSP, CISM, CRISC, CISA, ISO 27001 LA/ LI, ISO 27701 or equivalent.

For Cloud: ISO/IEC 27017, CCSP or equivalent.

For OT: ISA/IEC 62443 or equivalent

Senior Consultant Criteria

Educational and Experience Requirements

An Senior Consultant must:

Hold a bachelor's degree in Computer Science, Information Technology, Cyber Security, Information Security, or an equivalent field and possess at least 8 years of total IT and information security experience. Out of this, a minimum of 5 years should specifically be in cyber security and at least 3 years must involve experience in fields like GRC, Risk assessments, security/ compliance audits, vulnerability assessments/penetration testing.

Or

Hold MS/ PhD in Information/ Cyber Security or related field and possess at least 5 years of total IT and information security experience. Out of this, a minimum of 4 years should specifically be in cyber security and at least 3 years must involve experience in fields like GRC, Risk assessments, security/ compliance audits, vulnerability assessments/penetration testing.

And

Must Possess an experience of at least 7 Audits or Compliance preparedness engagement, gap assessments, risk assessments.

Core Certifications

The consultant must hold at least two certifications, one Certifications like: CISSP, CISM, CRISC, CISA, ISO 27001 LA/ LI or equivalent

And one certification based on domain expertise:

For IT: CISSP, CISM, CRISC, CISA, ISO 27001 LA/ LI, ISO 27701 or equivalent.

For Cloud: ISO/IEC 27017, CCSP or equivalent.

For OT: ISA/IEC 62443 or equivalent

Assessment / Test Requirement (In Future)

The consultant should qualify the prescribed evaluation or competency test of GRC specifically focused on PISF that will be conducted by nCERT or any accredited body of nCERT.

Note: Details about the competency test will be provided once the process will be initiated.

Junior Consultant Criteria

Educational and Experience Requirements

A junior Consultant must:

Hold a bachelor's degree in Computer Science, Information Technology, Cyber Security, Information Security, or an equivalent field and possess at least 3 years of total IT and information security experience. Out of this, a minimum of 2 years should specifically be in fields like GRC, Risk assessments, security/ compliance audits, vulnerability assessments/penetration testing.

Or

Hold MS/ PhD in Information/ Cyber Security or related field and possess at least 2 years of information security experience in fields like GRC, Risk assessments, security/ compliance audits, vulnerability assessments/penetration testing.

And

Must Possess an experience of at least 5 Audits or Compliance preparedness engagement, gap assessments, risk assessments, VA or PT.

Core Certifications

The consultant must hold at least one certification like ISO 27001 LA/LI, CEH, OSCP, Security+, GIAC or equivalent.