# QUALIFICATION FILE

## Network Security Engineer

☒ Short Term Training (STT) ☐ Long Term Training (LTT) ☐ Apprenticeship

☒ Upskilling ☐ Dual/Flexi Qualification ☐ For ToT

☐ For ToA

☐General ☐ Multi-skill (MS) ☐ Cross Sectoral (CS) ☒ Future Skills ☐ OEM

**NCrF/NSQF Level: 6**

**Submitted By:**

**IT-ITeS Sector Skills Council NASSCOM (SSC NASSCOM)**
**Plot No. – 7, 8, 9 & 10**
**Sector – 126, Noida, Uttar Pradesh - 201303**

# Table of Contents

# Section 1: Basic Details

| | | | |
|---|---|---|---|
| **1.** | **Qualification Name** | **Network Security Engineer** | |
| **2.** | **Sector/s** | **IT/ITeS** | |
| **3.** | **Type of Qualification: ☐ New ☒ Revised ☐ Has Electives/Options ☐ OEM** | **NQR Code & version of the existing /previous qualification:** *QG-05-IT-01559-2023-V1.1-NASSCOM and Version 3* | **Qualification Name of the existing/previous version: Consultant Network Security** |
| **4.** | **Qualification Name** *(Wherever applicable)* | ***Network Security Engineer*** | |
| **5.** | **National Qualification Register (NQR) Code &Version** (*Will be issued after NSQC approval*) | ***QG-06-IT-045872025-V2-NASSCOM and Version 4*** | **6. NCrF/NSQF Level:6** |
| **7.** | **Award (Certificate/Diploma/Advance Diploma/ Any Other** *(Wherever applicable specify multiple entry/exits also & provide details in annexure)* | Certificate | |
| **8.** | **Brief Description of the Qualification** | The qualification presents a comprehensive approach to network security and compliance management, designed to equip individuals with the essential skills and knowledge required to protect organizational information systems. It encompasses a wide range of topics, including foundational concepts of network security, risk management, compliance with regulatory standards (such as GDPR and PCI-DSS), and practical implementation of security measures like firewalls and intrusion detection systems. Participants engage in evaluating existing security postures, conducting audits, and understanding stakeholder roles in cybersecurity practices. Additionally, the qualification emphasizes hands-on experience with industry-standard tools and software, preparing individuals for real-world challenges in safeguarding digital assets and maintaining regulatory compliance. Overall, this qualification aims to cultivate adept cybersecurity professionals who can effectively contribute to their organizations' security frameworks. | |

<table>
<tr><td>9.</td><td>Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee</td><td colspan="2">a. Entry Qualification & Relevant Experience:<br>*Relevant Experience in job roles related to IT/Computer Science/Cybersecurity<br>The relevant experience would include work, internship and apprenticeship after completing relevant educational qualifications.<br>** PG or UG or diploma with courses related to Engg./ Science<br><br>
<table>
<tr><th>S. No.</th><th>Academic/Skill Qualification (with Specialization - if applicable)</th><th>Required Experience (with Specialization - if applicable)</th></tr>
<tr><td>1</td><td>Completed 4th year UG**</td><td>-</td></tr>
<tr><td>2</td><td>Previous Relevant qualification of NSQF level 5.5</td><td>1.5 years of relevant experience*</td></tr>
<tr><td>3</td><td>Previous Relevant qualification of NSQF level 5</td><td>3 years of relevant experience*</td></tr>
</table>
b. Age: NA</td></tr>
<tr><td>10.</td><td>Credits Assigned to this Qualification, Subject to Assessment (as per National Credit Framework (NCrF))</td><td>20 Credits</td><td>11. Common Cost Norm Category (I/II/III) (wherever applicable): II</td></tr>
<tr><td>12.</td><td>Any Licensing Requirements for Undertaking Training on This Qualification (wherever applicable)</td><td colspan="2">NA</td></tr>
<tr><td>13.</td><td>Training Duration by Modes of Training Delivery (Specify Total Duration as per selected training delivery modes and as per requirement of the qualification)</td><td colspan="2">☐ Offline Only ☐ Online Only ☒ Blended<br><br>
<table>
<tr><th>Training Delivery Mode</th><th>Theory (Hours)</th><th>Practical (Hours)</th><th>OJT (Mandatory) Hours</th><th>OJT (Recommended) Hours</th><th>Total (Hours)</th></tr>
<tr><td>Classroom (offline)</td><td>176</td><td>304</td><td>120</td><td></td><td>600</td></tr>
<tr><td>Online</td><td>176</td><td>304</td><td>120</td><td></td><td>600</td></tr>
</table>
(Refer Blended Learning Annexure for details)</td></tr>
<tr><td>14.</td><td>Aligned to NCO/ISCO Code/s (if no code is available mention the same)</td><td colspan="2">NCO-2015/ NIL</td></tr>
</table>

| | | | |
|---|---|---|---|
| **15.** | **Progression Path After Attaining the Qualification, wherever applicable** *(Please show Professional and Academic progression)* | This entry should refer to one or more of the following:<br>**Professional progression**: Access to related qualification(s) at the next NSQF level –Senior Consultant- Network Security, Lead Penetration Tester, Forensics Specialist, Architect- App Security, etc.<br>**Academic progression**: Access to other qualifications at the same NSQF level - Penetration Tester, Senior Security Analyst, Senior Analyst- App Security, etc. | |
| **16.** | **Other Indian languages in which the Qualification & Model Curriculum are being submitted** | Hindi | |
| **17.** | **Is similar Qualification(s) available on NQR-if yes, justification for this qualification** | **☐ Yes ☒ No URLs of similar Qualifications:** | |
| **18.** | **Is the Job Amenable to Persons with Disability** | **☐ Yes ☒ No**<br>**If "Yes", specify applicable type of Disability:** | |
| **19.** | **How participation of women will be encouraged?** | The Program is gender neutral although to increase the women participation, organizations are keeping aside few seats to encourage the female candidates | |
| **20.** | **Are Greening/Environment Sustainability Aspects covered** (*Specify the NOS/Module which Covers it)* | **☒ Yes ☐ No, DGT/VSQ/N0102:** Employability Skill (60 Hours) | |
| **21.** | **Is Qualification suitable to be offered in Schools/Colleges** | **Schools: ☐ Yes ☒ No Colleges ☒ Yes ☐ No** | |
| **22.** | **Name and Contact Details Submitting / Awarding Body SPOC** *(In case of CS or MS, provide details of both Lead AB & Supporting ABs)* | **Name: Namrata Kapur**<br>**Email: Standards@nasscom.in**<br>**Contact No.: 0120-4990111**<br>**Website: https://www.sscnasscom.com/** | |
| **23.** | **Final Approval Date by NSQC: 07th October 2025** | **24. Validity Duration: 3 Years** | **25. Next Review Date: 07th October 2028** |

# Section 2: Module Summary

## NOS/s of Qualifications

*(In exceptional cases these could be described as components)*

### Mandatory NOS/s:

Specify the training duration and assessment criteria at NOS/Module level. For Further details refer curriculum document.

**Th.**-Theory **Pr.**-Practical **OJT**-On the Job training **Man.**-Mandatory Training **Rec.**-Recommended **Proj.-** Project

| S. No | NOS/Module Name | NOS/Module Code & Version *(if applicable)* | Core/ Non-Core | NCrF/NSQF Level | Credits as per NCrF | Training Duration (Hours) | | | | | Assessment Marks | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Th. | Pr. | OJT-Man. | OJT-Rec. | Total | Th. | Pr. | Proj. | Viva | Total | Weightage (%) (if applicable) |
| 1. | Maintain compliance to information security policies, regulations and standards and address risk issues. | SSC/N0918, V3.0 | Core | 6 | 04 | 40:00 | 50:00 | 30:00 | 00:00 | 120:00 | 30 | 50 | - | 20 | 100 | 18% |
| 2. | Conduct network security assessment and provide recommendations as per requirements | SSC/N0922, V3.0 | Core | 6 | 05 | 41:00 | 79:00 | 30:00 | 00:00 | 150:00 | 30 | 50 | - | 20 | 100 | 18% |

| S. No | NOS/Module Name | NOS/Module Code & Version *(if applicable)* | Core/ Non-Core | NCrF/NSQF Level | Credits as per NCrF | Training Duration (Hours) | | | | | Assessment Marks | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Th. | Pr. | OJT-Man. | OJT-Rec. | Total | Th. | Pr. | Proj. | Viva | Total | Weightage (%) (if applicable) |
| 3. | Carry out configuration review and provide recommendations to support in remediating the identified vulnerabilities | SSC/N0923, V3.0 | Core | 6 | 05 | 40:00 | 80:00 | 30:00 | 00:00 | 150:00 | 30 | 50 | - | 20 | 100 | 18% |
| 4. | Test, run exploits to identify vulnerabilities in networks | SSC/N0925, V3.0 | Core | 6 | 03 | 25:00 | 50:00 | 15:00 | 00:00 | 90:00 | 30 | 50 | - | 20 | 100 | 18% |
| 5. | Foster collaboration between various stakeholders to ensure cohesive cybersecurity practices across the organization. | SSC/N0927, V3.0 | Core | 6 | 01 | 06:00 | 09:00 | 15:00 | 00:00 | 30:00 | 30 | 50 | - | 20 | 100 | 18% |
| 6. | Employability Skills (60 Hours) | DGT/VSQ/N0102, V1.0 | Non-Core | 4 | 02 | 24:00 | 36:00 | 00:00 | 00:00 | 60:00 | 20 | 30 | - | - | 50 | 10% |
| **Duration (in Hours)/Total Marks** | | | | | **20** | **176:00** | **304:00** | **120:00** | **00:00** | **600:00** | **170** | **280** | **-** | **100** | **550** | **100** |

### Elective NOS/s:

| S. No | NOS/Module Name | NOS/Module Code & Version *(if applicable)* | Core/ Non-Core | NCrF/NSQF Level | Credits as per NCrF | Training Duration (Hours) | | | | | Assessment Marks | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Th. | Pr. | OJT-Man. | OJT-Rec. | Total | Th. | Pr. | Proj. | Viva | Total | Weightage (%) *(if applicable)* |
| 1. | | | | | | | | | | | | | | | | |
| 2. | | | | | | | | | | | | | | | | |
| **Duration (in Hours) / Total Marks** | | | | | | | | | | | | | | | | |

### Optional NOS/s:

| S. No | NOS/Module Name | NOS/Module Code & Version *(if applicable)* | Core/ Non-Core | NCrF/NSQF Level | Credits as per NCrF | Training Duration (Hours) | | | | | Assessment Marks | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Th. | Pr. | OJT-Man. | OJT-Rec. | Total | Th. | Pr. | Proj. | Viva | Total | Weightage (%) *(if applicable)* |
| 1. | | | | | | | | | | | | | | | | |
| 2. | | | | | | | | | | | | | | | | |
| **Duration (in Hours) / Total Marks** | | | | | | | | | | | | | | | | |

## Assessment - Minimum Qualifying Percentage

**Assessment - Minimum Qualifying Percentage**
**Minimum Pass Percentage – Aggregate at qualification level: 70 %** (Every Trainee should score specified minimum aggregate passing percentage at qualification level to successfully clear the assessment.)



# Section 3: Training Related

| | | |
|---|---|---|
| 1. | **Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)* | **Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science) |

| | | |
|---|---|---|
| | | **Industry & training experience:** 2 years of industry experience in Cybersecurity. The industry experience would include work, internship, and apprenticeship undertaken after regular graduation<br><br>**Certification:** "Trainer" mapped to the Qualification Pack "MEP/Q2601" Minimum accepted score is 80% aggregate |
| 2. | **Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)* | **Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science)<br><br>**Industry & training experience:** 4 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation.<br><br>**Certification:** "Master Trainer" mapped to the Qualification Pack "MEP/Q2602" Minimum accepted score is 90% aggregate |
| 3. | **Tools and Equipment Required for the Training** | ☒Yes ☐No *(If "Yes", details to be provided in Annexure)* |
| 4. | **In Case of Revised Qualification, details of Any Upskilling Required for Trainer** | NA |

# Section 4: Assessment Related

| | | |
|---|---|---|
| 1. | **Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)* | **Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science)<br><br>**Industry & Training Experience:** 2 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation.<br><br>**Certification:** "Assessor" mapped to the Qualification Pack "MEP/Q2701" Minimum accepted score is 80% aggregate. |
| 2. | **Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines), (wherever applicable)* | **Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science)<br><br>**Industry & Training Experience:** 2 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation.<br><br>**Certification:** "Assessor" mapped to the Qualification Pack "MEP/Q2701" Minimum accepted score is 80% aggregate. |

| | | |
|---|---|---|
| 3. | **Lead Assessor's/Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)* | **Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science)<br><br>**Industry & Training Experience:** 4 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation.<br><br>**Certification:** "Lead Assessor" mapped to the Qualification Pack "MEP/Q2702" Minimum accepted score is 90% aggregate. |
| 4. | **Assessment Mode** *(Specify the assessment mode)* | The assessment will consist of a blend of hands-on practical evaluations, viva-voce, and online proctored scenario-based multiple-choice questions ensuring a thorough evaluation of the individual's proficiency in learning outcomes, practical understanding, and real-world application of concepts. |
| 5. | **Tools and Equipment Required for Assessment** | ☒ Same as for training ☐ Yes ☐ No *(details to be provided in Annexure-if it is different for Assessment)* |

## Section 5: Evidence of the Need for Qualification

*Provide Annexure/Supporting documents name.*

| | |
|---|---|
| 1. | Latest Skill Gap study (not older than 2 years) (Yes/No): Yes |
| 2. | Latest Market Research Reports or any other source (not older than 2 years) (Yes/No): Yes |
| 3. | Government/Industry initiatives/requirement (Yes/No): Industry Initiatives |
| 4. | Number of industry validations provided: 21 |
| 5. | Estimated number of people to be trained and employed: NA |
| 6. | Evidence of Concurrence/Consultation with Line/State Departments:<br><br>If "No", why: |

## Section 6: Annexure & Supporting Documents Check List

*Specify Annexure Name / Supporting document file name*

| | | |
|---|---|---|
| 1. | **Annexure:** NCrF/NSQF level justification based on NCrF/NSQF descriptors *(Mandatory)* | Evidence of Level |
| 2. | **Annexure:** List of tools and equipment relevant for NOS *(Mandatory, except in case of online course)* | Tools and Equipment (lab set-up) |
| 3. | **Annexure:** Detailed Assessment criteria *(Mandatory)* | Performance Criteria Details |
| 4. | **Annexure:** Assessment Strategy *(Mandatory)* | Assessment Strategy |
| 5. | **Annexure:** Blended Learning *(Mandatory, in case selected Mode of delivery is Blended Learning)* | NA |
| 6. | **Annexure:** Multiple Entry Exit Details *(Mandatory, in case qualification has multiple entry-exit)* | Acronym and Glossary |
| 7. | **Annexure:** Acronym and Glossary *(Optional)* | Acronym and Glossary |
| 8. | **Supporting Document:** Model Curriculum *(Mandatory-Public View)* | MC_SSCQ0917_Consultant network security_V4 |
| 9. | **Supporting Document:** Career Progression *(Mandatory-Public View)* | Occupational Map-Cybersecurity |
| 10. | **Supporting Document:** Occupational Map *(Mandatory)* | Occupational Map-Cybersecurity |
| 11. | **Supporting Document:** Assessment SOP *(Mandatory)* | NA |
| 12. | **Any Other document you wish to submit:** | NA |



## Annexure: Evidence of Level

| NCrF/NSQF Level Descriptors | Key requirements of the job role/ outcome of the qualification | How the job role/ outcomes relate to the NCrF/NSQF level descriptor | NCrF/NSQF Level |
|---|---|---|---|
| **Professional Theoretical Knowledge/Process** | **Provide network security recommendations as per requirements**<br>• Evaluate the existing network protocols and topology of users<br>• consult with engineering teams engaged in IT networking and network security to | The job role demands a wide range of specialised technical skill sets in the network security domain, as Network Consultant essentially acts as the technical advisor to be able to provide organizations with necessary recommendations in | 6 |

| NCrF/NSQF Level Descriptors | Key requirements of the job role/ outcome of the qualification | How the job role/ outcomes relate to the NCrF/NSQF level descriptor | NCrF/NSQF Level |
|---|---|---|---|
| | identify network security vulnerabilities and requirements<br>• research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities, and security risks<br>• explore potential vulnerabilities that could be technical, operational or management related<br>• research options of network security solutions that match the productivity and security requirements captured<br>• prepare recommendations that have the potential to meet the security objectives of the organisation<br>• provide the organisation with considered advice on the implications of accepting, modifying, or rejecting security recommendations<br>• co-ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs<br>**Carry out configuration review and provide recommendations for secure configuration of networks and security devices** | implementing suitable network security protocols for their IT infrastructures.<br>The job holder needs to have a strong expertise in a wide range of technical contexts relevant for network security, like analysing business requirements and priorities, existing network standards, risks faced by the organisation, knowledge of advanced networking technologies and devices, and ability to suggest ways to secure network security. | |

| NCrF/NSQF Level Descriptors | Key requirements of the job role/ outcome of the qualification | How the job role/ outcomes relate to the NCrF/NSQF level descriptor | NCrF/NSQF Level |
|---|---|---|---|
| | • provide recommendations for secure configuration measures for networks considering business requirements<br>• establish a baseline configuration that represents a secure state which is also cost-effective as supportive of business requirements<br>• provide recommendation for secure configuration policies and procedures in alignment to cyber security posture of the organization and business requirements<br>• suggest remediation actions to resolve issues caused due to erroneous network device configurations<br>**Test, run exploits to identify vulnerabilities in networks**<br>• test the network devices by supplying invalid inputs, random strings, etc., and check for any errors or unintended behaviour in the output<br>• find exploits e.g., proof-of-concept exploit for the various vulnerabilities found<br>• identify weak entry points and high value target assets of the organization or its network | | |

| NCrF/NSQF Level Descriptors | Key requirements of the job role/ outcome of the qualification | How the job role/ outcomes relate to the NCrF/NSQF level descriptor | NCrF/NSQF Level |
|---|---|---|---|
| | • demonstrate various possible impacts, compromises and exposures using specialized exploitation tools<br>• evaluate ways & means of identifying and closing weaknesses in the network<br>• recommend hardening measures for network security devices for minimizing exposure and vulnerabilities | | |
| **Professional and Technical Skills/ Expertise/ Professional Knowledge** | • basic cyber security concepts<br>• security methodologies and vulnerability frameworks<br>• relevant networking concepts, devices, and terminology<br>• knowledge of different cyber attacks<br>• network security principles and processes<br>• network security tools, technologies, and applications<br>• firewall management suits, incident management software and SIEM tools<br>• various sources for researching for existing network security solution<br>• categorization and root cause analysis process of vulnerabilities<br>• basics of enterprise information technology (IT) architecture<br>• secure integration approach with different third-party systems | Further the job role holder needs to research for solutions available as per the requirements, that would suit the organisation. This requires them to be up to date with the latest technologies in the market and perform extensive research across different facets of enterprise infrastructure and network security around new-age networking concepts, advanced network firewalls, dynamic load-balancing, automated traffic routing and switching, advanced incident management and vulnerability assessment. The job role holder needs to be factually and theoretically strong in his research and recommendations within the above mentioned conexts. | 6 |

| NCrF/NSQF Level Descriptors | Key requirements of the job role/ outcome of the qualification | How the job role/ outcomes relate to the NCrF/NSQF level descriptor | NCrF/NSQF Level |
|---|---|---|---|
| | • statutory knowledge (IT Act, TRAI Guidelines, and other national and international Guidelines)<br>• standards and industry best practices for network security<br>• new technological developments in Network security<br>• server administration and systems engineering theories, concepts, and methods Systems Life Cycle<br>• Segregation of Duties (SoD) configuration<br>• migration of systems and users<br>• the basic functionalities of theapplications, hardware and/or access rights that are used by the customers<br>• host/network access controls (e.g., access control list)<br>• Advanced knowledge of cloud security | | |
| **Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill** | • consult with customers to evaluate functional requirements for network security<br>• consult with engineering teams engaged in IT networking and network security to identify network security vulnerabilities and requirements<br>• identify and determine the cost, potential benefits, and effectiveness of | The job role primarily assesses the business impact due to the change or implementation of new networking technologies or infrastructure components on a broader perspective, and hence to carry-out multiple technological evaluations, benchmarking activities to help organizations employ the right networking standards. This require strong cognitive thinking and practical skills | 6 |

| NCrF/NSQF Level Descriptors | Key requirements of the job role/ outcome of the qualification | How the job role/ outcomes relate to the NCrF/NSQF level descriptor | NCrF/NSQF Level |
|---|---|---|---|
| | recommended security solutions, based on valid assumptions, considerations, and information, including possible constraints<br>• co-ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs<br>• take account of the organisation's values, culture, and nature of business<br>• advise stakeholders of difficulties or where it will be impossible to fulfil agreed actions in line with the terms of any agreements made<br>• communicate the compliance audit and risk assessment results to specified organizational personnel<br>• plan and coordinate the operational activities of a given company or organization to guarantee compliance with governmental regulations and ordinances<br>• ensure that customer needs are met within SLA and meet other time and quality commitment KPIs<br>• identify the business functions, and key stakeholders within these, and establish their interest and understanding, | to recommend solutions for specific problems in network security. | |

| NCrF/NSQF Level Descriptors | Key requirements of the job role/ outcome of the qualification | How the job role/ outcomes relate to the NCrF/NSQF level descriptor | NCrF/NSQF Level |
|---|---|---|---|
| | relevant to achieving the organisation's aims<br>• take agreements and track actionable of other functions for interrelated work<br>• ensure the allocation and authorisation of work to the project management team is consistent with achieving the project objectives | | |
| **Broad Learning Outcomes/Core Skill** | • provide the organisation with considered advice on the implications of accepting, modifying, or rejecting security recommendations | Network Consultant enables security professionals to perform various network security testing methods and model vulnerability scanning, intrusion detection and prevention, and threat monitoring systems, by leveraging extremely good mathematical calculation and logical skills. | 6 |
| **Responsibility** | • take account of the organisation's values, culture, and nature of business<br>• clarify architectural design to the implementation team<br>• provide inputs for implementation strategies and plan to the implementation team(s)<br>• perform comparative analysis and evaluation of the implemented solutions against architectural design<br>• suggest integration and interfaces for market/in-house solutions with other security solutions like SIEM or external solutions | They will also need to work in collaboration with stakeholders that range from Business heads to Security teams, IT teams, users, vendors, specialists in order to understand their needs, customize solutions, communicate risk and processes that need to be followed to the teams, resolve queries regarding the solution, etc. This requires a person with good communication and interpersonal skills.<br><br>All this work warrants significant data collection, analysis, and commination skills to effectively advise and convince the customers and stakeholders in general. | 6 |

| NCrF/NSQF Level Descriptors | Key requirements of the job role/ outcome of the qualification | How the job role/ outcomes relate to the NCrF/NSQF level descriptor | NCrF/NSQF Level |
|---|---|---|---|
| | • review the implementation steps and their outcome to ensure that they satisfy architectural objectives and adhere to design<br>• assess how implementation satisfies compliance requirements<br>• ensure technology risk considerations are identified and adequately addressed for new application developments, integration, and deployment | | |



## Annexure: Tools and Equipment (lab set-up)

List of Tools and Equipment

**Batch Size:**

| S. No. | Tool / Equipment Name | Specification | Quantity for specified Batch size |
|---|---|---|---|
| 1 | PC/Laptop with internet | - | |
| 2 | Network Protocol Analyzer | Wireshark | |
| 3 | Open-source Firewall | pfSense | |
| 4 | Vulnerability Scanner | OpenVAS | |
| 5 | Risk Assessment Tool | OpenSCAP | |
| 6 | Configuration Management Tool | Ansible | |
| 7 | Security Auditing Tool | Lynis | |
| 8 | Penetration Testing Framework | Metasploit Community Edition | |
| 9 | Network Scanner | Nmap | |
| 10 | Web Application Scanner | Nikto | |
| 11 | Data Encryption Tool | GPG (GNU Privacy Guard) | |
| 12 | Compliance Checker | CloudSploit | |
| 13 | Documentation Management | Google Docs | |

*Tools are open source

Classroom Aids

The aids required to conduct sessions in the classroom are:

1. White Board
2. White Board Marker
3. Projector

## Annexure: Industry Validations Summary

Provide summary information of all the industry validation in table. This is not required for OEM Qualifications.

| S. No | Organization Name | Representative Name | Designation | Contact Address | Contact Phone No | E-mail ID | LinkedIn Profile (if available) |
|---|---|---|---|---|---|---|---|
| 1 | Renew | Aseem Mukhi | Chief Information Security Officer | - | 9990002658 | assem.mukhi@gmail.com | https://www.linkedin.com/in/aseem-mukhi-1544854/ |
| 2 | Sankey Solutions | Sobha Patil | CEO | - | 9008193344 | shobha@sankeysolutions.com | https://www.linkedin.com/in/shobhapatil/?originalSubdomain=in |
| 3 | Accolite Digital | Ayushmaan Pandey | Senior Software Engineer | - | 8077386365 | ayushmaan.pandey@accolitedigital.com | https://www.linkedin.com/in/ayushmaanpandey |
| 4 | Infosys | Vivek Pilaniya | Program Manager | - | 9718423687 | vivek.pilania@infosys.com | https://www.linkedin.com/in/vivekpilania-iimc |
| 5 | Data Switch | Thilak Hari A | Product Engineer | - | 6393798750 | thilakhariharan@gmail.com | https://www.linkedin.com/in/thilak-hariharasudhan-43a89b269/ |
| 6 | Forbes | Naveenkumar Janakiraman | Data Research Analyst | - | 9976773109 | naveenkumarj4997@gmail.com | https://www.linkedin.com/in/naveenkumar-janakiraman |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | S3V Vascular Technologies | Yeaswanth Raj V | Clinical Research Executive | - | 7502629955 | yeaswanthraj@gmail.com | - |
| 8 | Kornferry | Ragul Kumar | Data analyst | - | 9659964881 | ragul@kornferry.com | https://www.linkedin.com/in/ragul-kumar-b2297a171/ |
| 9 | Acolyte | Saranya | Research Analyst | - | 9944313170 | saranyakathir128@gmail.com | - |
| 10 | Frontier | Santhosh kumar S | DevOps L1 | - | 9655747400 | santhoshselvaraj24031998@gmail.com | - |
| 11 | Amazon | Asvin Ragav R | Data Associate | - | 9994308478 | asvinragav16@gmail.com | - |
| 12 | Rndsoft | Tamilselvan | Software developer | - | 9361784871 | dtamilselvan1004@gmail.com | - |
| 13 | Intellibren | Kailash PD | Director | - | 6374700185 | kailash@intellibren.com | - |
| 14 | Mindshare (Inclusive Minds) | Pamindar Singh | Team Lead | - | 8713901984 | paminder.singh@themindshare.in | https://www.linkedin.com/in/paminder-singh-7990b8101/ |
| 15 | Iaccept software pvt ltd | B Mohan Kumar | Founder | - | 9845208784 | mohan@iaccept.in | https://www.linkedin.com/in/bmohankumar/?originalSubdomain=in |
| 16 | QAcadmey | Deepak Gour | Product and Academic Head | - | 9893554394 | deepak@qacademy.ca | https://ca.linkedin.com/in/deepak-gour-8853968 |
| 17 | TCS | Karthiga N | Test Analyst | - | 7092257551 | karthiga0115@gmail.com | - |
| 18 | Skillsda | Sankar Vijyan/Thiru R | Centre Manager/Head R&D | - | 9894801793 | sv@skillsda.com/thiru@skillsda.com | https://www.linkedin.com/in/sankar-vijayan-73a33852/ |
| 19 | Wipro | Narendra Nande | Director | - | 9900086708 | narendra.nande@wipro.com | https://www.linkedin.com/in/narendra-nande-84402a2/?originalSubdomain=in |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 20 | Barq | Satheesh Sekar | Senior Decision Scientist | - | 9444218513 | satheeshk.sekar@gmail.com | https://www.linkedin.com/in/satheeshksekar/?originalSubdomain=in |
| 21 | Neoquant | Rishi Agrawal | Chief Technology Officer | - | 7702191049 | agrishi@gmail.com/Rishi.agarwal@neoquant.com | https://www.linkedin.com/in/agrishi/?originalSubdomain=in |

Annexure: Training & Employment Details

**Training & Employment Projections:**

| Year | Total Candidates | | Women | | People with Disability | |
|---|---|---|---|---|---|---|
| | Estimated Training # | Estimated Employed Opportunities | Estimated Training # | Estimated Employed Opportunities | Estimated Training # | Estimated Employed Opportunities |
| | | | | | | |

Data to be provided year-wise for next 3 years.

**Training, Assessment, Certification, and Placement Data for previous versions of qualifications:**

| Qualification Version | Year | Total Candidates | | | Women | | | People with disability | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Trained | Assessed | Certified | Trained | Assessed | Certified | Trained | Assessed | Certified |
| | | | | | | | | | | |
| | | | | | | | | | | |

Applicable for revised qualifications only; data to be provided year-wise for the next 3 years.

**List Schemes in which the previous version of qualification was implemented**:

1.

**Content availability for the previous version of qualifications:**

☐ Participant Handbook ☐ Facilitator Guide ☐ Digital Content ☐ Qualification Handbook ☐ Any Other:

**Language in which content is available:**

# Annexure: Blended Learning

**Blended Learning Estimated Ratio & Recommended Tools:**

***Refer NCVET "Guidelines for Blended Learning for Vocational Education, Training & Skilling" available on:***
*https://ncvet.gov.in/sites/default/files/Guidelines%20for%20Blended%20Learning%20for%20Vocational%20Education,%20Training%20&%20Skilling.pdf*

| S. No. | Select the Components of the Qualification | List Recommended Tools – for all Selected Components | Offline: Online Ratio |
|---|---|---|---|
| 1 | ☐Theory/ Lectures - Imparting theoretical and conceptual knowledge | NA | NA |
| 2 | ☐Imparting Soft Skills, Life Skills, and Employability Skills /Mentorship to Learners | NA | NA |
| 3 | ☐Showing Practical Demonstrations to the learners | NA | NA |
| 4 | ☐Imparting Practical Hands-on Skills/ Lab Work/ workshop/ shop floor training | NA | NA |
| 5 | ☐Tutorials/ Assignments/ Drill/ Practice | NA | NA |
| 6 | ☐Proctored Monitoring/ Assessment/ Evaluation/ Examinations | NA | NA |
| 7 | ☐On the Job Training (OJT)/ Project Work Internship/ Candidate Training | NA | NA |

# Annexure: Detailed Assessment Criteria

Detailed Assessment criteria for each NOS/Module are as follows:

| NOS/Module Name | Assessment Criteria for Performance Criteria/Learning Outcomes | Theory Marks | Practical Marks | Project Marks | Viva Marks |
|---|---|---|---|---|---|
| SC/N0918 (Maintain compliance to information security policies, regulations and standards and address risk issues in organisations | PC1. Communicate compliance audit and risk assessment results to relevant personnel. | 2 | 3 | - | 1 |
| | PC2. Identify and share compliance issues found during audits with appropriate personnel. | 2 | 3 | - | 1 |
| | PC3. Plan and coordinate organizational activities to ensure compliance with regulations and standards. | 2 | 3 | - | 1 |
| | PC4. Document and implement all policies and procedures effectively. | 2 | 3 | - | 1 |
| | PC5. Conduct internal reviews to identify compliance issues and initiate corrective actions. | 2 | 4 | - | 2 |
| | PC6. Submit compliance reports to regulatory bodies. | 2 | 4 | - | 2 |
| | PC7. Monitor risk factors in organizational operations and take necessary corrective actions. | 3 | 5 | - | 2 |
| | PC8. Present identified compliance issues to management for prioritization and risk mitigation. | 3 | 5 | - | 2 |
| | PC9. Maintain regular communication with various stakeholders to coordinate compliance activities. | 3 | 5 | - | 2 |
| | PC10. Document all processes and outcomes for audits. | 3 | 5 | - | 2 |
| | PC11. Utilize AI-driven tools for continuous monitoring of compliance and risk assessment. | 3 | 5 | - | 2 |
| | PC12. Implement cloud-based compliance management solutions to streamline reporting and documentation. | 3 | 5 | - | 2 |
| | **Total Marks** | **30** | **50** | **-** | **20** |
| SSC/N0922 (Conduct network security assessment and provide recommendations as per requirements) | PC1. Consult with clients to understand functional requirements for network security. | 3 | 5 | - | 2 |
| | PC2. Define project objectives based on customer requirements and existing security measures. | 3 | 5 | - | 2 |
| | PC3. Evaluate current network protocols, topology, and existing security measures. | 3 | 5 | - | 2 |

| NOS/Module Name | Assessment Criteria for Performance Criteria/Learning Outcomes | Theory Marks | Practical Marks | Project Marks | Viva Marks |
|---|---|---|---|---|---|
| | PC4. Conduct risk analysis and threat identification related to network security. | 3 | 5 | - | 2 |
| | PC5. Identify and document security vulnerabilities and constraints that may impact the organization. | 3 | 5 | - | 2 |
| | PC6. Research and assess potential security solutions based on organizational needs. | 3 | 5 | - | 2 |
| | PC7. Prepare comprehensive recommendations that address security objectives, considering costs and benefits. | 3 | 5 | - | 2 |
| | PC8. Maintain confidentiality of sensitive information during the analysis and recommendation process. | 3 | 5 | - | 2 |
| | PC9. Assess the security of cloud environments and provide recommendations for cloud security policies. | 3 | 5 | - | 2 |
| | PC10. Incorporate AI techniques to analyze historical security incident data for improved risk assessment. | 3 | 5 | - | 2 |
| | **Total Marks** | **30** | **50** | **-** | **20** |
| SSC/N0923 (Carry out configuration review and provide recommendations to support in remediating the identified vulnerabilities) | PC1. Conduct an inventory of network items requiring security configuration. | 3 | 5 | - | 2 |
| | PC2. Review configurations of identified items for security vulnerabilities. | 3 | 5 | - | 2 |
| | PC3. Provide recommendations for secure configurations aligning with organizational business needs. | 3 | 5 | - | 2 |
| | PC4. Test configurations prior to implementation, diagnosing and addressing issues as needed. | 3 | 5 | - | 2 |
| | PC5. Perform vulnerability assessments using various methodologies and tools to identify weaknesses. | 3 | 6 | - | 2 |
| | PC6. Recommend hardening measures for network devices to minimize vulnerabilities. | 3 | 6 | - | 2 |
| | PC7. Document all assessments and configurations for future reference and compliance. | 4 | 6 | - | 2 |
| | PC8. Implement cloud security configuration standards to ensure secure setups in cloud environments. | 4 | 6 | - | 3 |
| | PC9. Utilize AI tools for automated vulnerability scanning and threat detection in network configurations. | 4 | 6 | - | 3 |
| | **Total Marks** | **30** | **50** | **-** | **20** |

| NOS/Module Name | Assessment Criteria for Performance Criteria/Learning Outcomes | Theory Marks | Practical Marks | Project Marks | Viva Marks |
|---|---|---|---|---|---|
| SSC/N0925 (Test, run exploits to identify vulnerabilities in networks) | PC1. gather preliminary information by manually reviewing the documentation, secure coding policies, security requirements, architectural designs, | 1 | 2 | - | 1 |
| | PC2. gather network information using various information gathering methods and tools | 1 | 2 | - | 1 |
| | PC3. define scope for the tests using Existing Security Policies & Industry Standards | 1 | 2 | - | 1 |
| | PC4. plan for the test while adhering to business and time constraints put by organization | 1 | 2 | - | 1 |
| | PC5. perform Active Reconnaissance on the target network using metadata, search engines, social engineering, dumpster diving etc. after taking adequate approvals | 1 | 2 | - | 1 |
| | PC6. develop a map of target environments | 1 | 2 | - | 1 |
| | PC7. utilize network infrastructure scanning tool to conduct comprehensive network sweeps, port scans, Operating System fingerprinting and version scanning | 1 | 2 | - | 1 |
| | PC8. identify live systems, open / filtered ports found, services running on these ports, mapping router / firewall rules, operating system details, network path discovery, etc. | 1 | 2 | - | 1 |
| | PC9. perform fingerprinting services running behind open ports and underlying operating system | 1 | 2 | - | 1 |
| | PC10. explore the network by pre-determined scans to find possible vulnerabilities | 1 | 2 | - | 1 |
| | PC11. perform social engineering using Social Engineering Toolkit SET to find possible security holes | 2 | 3 | - | 1 |
| | PC12. test the network devices by supplying invalid inputs, random strings, etc., and check for any errors or unintended behaviour in the output | 2 | 3 | - | 1 |
| | PC13. find exploits e.g. proof-of-concept exploit for the various vulnerabilities found | 2 | 3 | - | 1 |
| | PC14. identify weak entry points and high value target assets of the organization or its network | 2 | 3 | - | 1 |
| | PC15. identify antiviruses e.g. host-based intrusion prevention systems, web application firewalls, and other preventative technologies in the system | 2 | 3 | - | 1 |
| | PC16. use pivoting techniques through targeted systems | 2 | 3 | - | 1 |

| NOS/Module Name | Assessment Criteria for Performance Criteria/Learning Outcomes | Theory Marks | Practical Marks | Project Marks | Viva Marks |
|---|---|---|---|---|---|
| | PC17. demonstrate various possible impacts, compromises and exposures using specialized exploitation tools | 2 | 3 | - | 1 |
| | PC18. evaluate ways & means of identifying and closing weaknesses in the network | 2 | 3 | - | 1 |
| | PC19. recommend hardening measures for network security devices for minimizing exposure and vulnerabilities | 2 | 3 | - | 1 |
| | PC20. maintain logs for all the activities performed | 2 | 3 | - | 1 |
| | **Total Marks** | **30** | **50** | **-** | **20** |
| SSC/N0927 (Foster collaboration between various stakeholders to ensure cohesive cybersecurity practices across the organization) | PC1. Identify key stakeholders and understand their roles and concerns in relation to cybersecurity. | 3 | 5 | - | 2 |
| | PC2. Create an inventory of cybersecurity-related operations and responsibilities. | 3 | 5 | - | 2 |
| | PC3. Collaborate with stakeholders to discuss key decisions impacting cybersecurity practices. | 3 | 5 | - | 2 |
| | PC4. Track and follow up on actionable items agreed upon with stakeholders. | 3 | 5 | - | 2 |
| | PC5. Monitor the effectiveness of interdepartmental relationships and seek feedback for improvement. | 3 | 6 | - | 2 |
| | PC6. Address conflicts of interest with stakeholders in a manner that minimizes disruption. | 3 | 6 | - | 2 |
| | PC7. Ensure agreements are fulfilled and communicate any potential difficulties promptly. | 4 | 6 | - | 2 |
| | PC8. Promote awareness of AI and cloud technologies among stakeholders regarding their impact on cybersecurity. | 4 | 6 | - | 3 |
| | PC9. Collaborate with cloud service providers to ensure compliance with established security standards. | 4 | 6 | - | 3 |
| | **Total Marks** | **30** | **50** | **-** | **20** |
| DGT/VSQ/N0102 Employability Skill(60 Hours) | PC1. Introduction to Employability Skills | 1 | 1 | - | - |
| | PC2. Constitutional values – Citizenship | 1 | 1 | - | - |
| | PC3. Becoming a Professional in the 21st Century | 2 | 4 | - | - |
| | PC4. Basic English Skills | 2 | 3 | - | - |
| | PC5. Career Development & Goal Setting | 1 | 2 | - | - |
| | PC6. Communication Skills | 2 | 2 | - | - |
| | PC7. Diversity & Inclusion | 1 | 2 | - | - |

| NOS/Module Name | Assessment Criteria for Performance Criteria/Learning Outcomes | | Theory Marks | Practical Marks | Project Marks | Viva Marks |
|---|---|---|---|---|---|---|
| | PC8. | Financial and Legal Literacy | 2 | 3 | - | - |
| | PC9. | Essential Digital Skills | 3 | 4 | - | - |
| | PC10. | Entrepreneurship | 2 | 3 | - | - |
| | PC11. | Customer Service | 1 | 2 | - | - |
| | PC12. | Getting Ready for Apprenticeship & Jobs | 2 | 3 | - | - |
| | **Total Marks** | | **20** | **30** | **-** | **-** |
| **Grand Total Marks** | | | **170** | **280** | **-** | **100** |

## Annexure: Assessment Strategy

**Assessment Process Overview**

**Batch Creation & Assessment Request:**

Training Providers (TP) or Training Centers (TC), including any other authorized partner of Ministry/ Department create batches / push batches on the SIDH portal. Assessment requests are submitted through the SIDH portal or via email or other media as authorized from time to time. For NON-SIDH schemes, assessment requests are received electronically or through respective State Skill Mission portals. TP/TC initiates the assessment request through the InSDMS portal and processes the payment (where applicable).

**Batch Alignment & Confirmation:**

Upon payment confirmation, batches are assigned to the Assessment Agency based on factors like:

- Assessment readiness
- Availability of certified assessors for the specific job role
- Assessment capping to an assessment agency as prescribed from time to time for an AB An email communication / prescribed mode communication is sent to TP/TC for confirmation of the assessment date, with IT-ITeS SSC in the loop. Once confirmation is received, the Assessment Agency designates a TOA-certified assessor to conduct or facilitate the assessment.
- Batches are only formed when the Qualification is active.

**Candidate Verification & Assessment Execution:**

Candidate details are verified and documented at the beginning of the assessment by a certified assessor. A Quality Assurance (QA) mechanism is enforced, requiring an undertaking from the TC. Regular feedback is collected from TP/TC to ensure continuous improvement.

**Evidence Collection & Validation:**

Proctors or assessors capture date/time-stamped and geo-tagged photographs of the assessment location during the process. Attendance is also ensured offline. A PC-wise result analysis is conducted to refine assessment standards.

**Monitoring & Compliance:**

Batch monitoring follows established protocols, ensuring adherence to assessment guidelines. Sample based surprise visits are conducted at TC locations during both training and assessments to verify compliance. This structured approach ensures transparency, quality control, and validation throughout the assessment process.

**Testing Environment:**

- Check the Assessment location, date and time
- If the batch size is more than 30, then there should be 2 Assessors.
- Check that the allotted time to the candidates to complete Theory & Practical Assessment is correct.

**Assessment Quality Assurance levels/Framework:**

IT-ITeS SSC nasscom is responsible for the development and periodic review of the question bank developed for a specific job role. We publish an openly accessible sample /model question paper on our website for all stakeholders. The quality of the Question Bank created by the assessment designer is validated by a Subject matter experts on the following parameters:

- Appropriateness of the Question Bank in terms of facts, data and information.
- Checks for grammar, spellings, scripting and formatting.
- The information provided should be specific enough to remove any ambiguity in answers/solutions to the question.
- Relevance – Assessing the topic well w.r.t. the job role.
- Check if the difficulty level of each question is as per the matrix.
- Check if the images used in the question are clear and relevant.
- All variables, symbols and abbreviations used must be declared.
- The correct answer option should be unique, and the options should not be overlapping

# Annexure: Acronym and Glossary

Acronym

| Acronym | Description |
|---|---|
| **AA** | Assessment Agency |
| **AB** | Awarding Body |
| **NCrF** | National Credit Framework |
| **NOS** | National Occupational Standard(s) |
| **NQR** | National Qualification Register |
| **NSQF** | National Skills Qualifications Framework |
| **OJT** | On Job Training |

Glossary

| Term | Description |
|---|---|
| **National Occupational Standards (NOS)** | NOS define the measurable performance outcomes required from an individual engaged in a particular task. They list down what an individual performing that task should know and also do. |
| **Qualification** | A formal outcome of an assessment and validation process which is obtained when a competent body determines that an individual has achieved learning outcomes to given standards |
| **Qualification File** | A Qualification File is a template designed to capture necessary information of a Qualification from the perspective of NSQF compliance. The Qualification File will be normally submitted by the awarding body for the qualification. |
| **Sector** | A grouping of professional activities based on their main economic function, product, service or technology. |