QUALIFICATION FILE – Standalone NOS

Foundations of Cybersecurity

☒ Horizontal/Generic ☒ Vertical/Specialization

☒ Upskilling ☐ Dual/Flexi Qualification ☐ For ToT ☐ For ToA

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

NCrF/NSQF Level: 4.5

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

<table>
<tr><td>1.</td><td>NOS</td><td colspan="2">Foundations of Cybersecurity</td></tr>
<tr><td>2.</td><td>Sector/s</td><td colspan="2">IT/ITeS</td></tr>
<tr><td>3.</td><td>Type of Qualification ☒ New ☐ Revised</td><td>NQR Code & version of the existing /previous qualification: (change to previous, once approved)</td><td>Qualification Name of the existing/previous version: (previous, once approved)</td></tr>
<tr><td>4.</td><td>National Qualification Register (NQR) Code & Version (Will be issued after NSQC approval.)</td><td>NG-4.5-IT-03790-2025-V1-NASSCOM & V1</td><td>5. NCrF/NSQF Level: 4.5</td></tr>
<tr><td>6.</td><td>Brief Description of the Standalone NOS</td><td colspan="2">This NOS describes the fundamentals of cybersecurity</td></tr>
<tr><td>7.</td><td>Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee</td><td colspan="2">a. Entry Qualification & Relevant Experience:
<table>
<tr><th>S.No.</th><th>Academic/Skill Qualification (with Specialization - if applicable)</th><th>Relevant Experience (with Specialization - if applicable)</th></tr>
<tr><td>1</td><td>Pursuing 1st Year of 3Y/4Y UG Program in STEM</td><td>-</td></tr>
<tr><td>2</td><td>Completed 1st year of 3Y/4Y UG Program in STEM</td><td>-</td></tr>
<tr><td>3</td><td>Passed Class 12th or equivalent in STEM</td><td>1.5 Years of relevant experience (including work, internship, and apprenticeship) in Cybersecurity</td></tr>
<tr><td>4</td><td>Previous relevant qualification of NSQF Level 4</td><td>1.5 Years of relevant experience (including work, internship, and apprenticeship) in Cybersecurity</td></tr>
</table>
b. Age: NA</td></tr>
<tr><td>8.</td><td>Credits Assigned to this NOS-Qualification, Subject to Assessment (as per National Credit Framework (NCrF))</td><td>1.5 Credits</td><td>9. Common Cost Norm Category (I/II/III) (wherever applicable): II</td></tr>
<tr><td>10.</td><td>Any Licensing Requirements for Undertaking Training on This Qualification (wherever applicable)</td><td colspan="2">NA</td></tr>
</table>

<table>
<tr><td>11.</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>☐ Offline Only ☐ Online Only ☒ Blended
<table><tr><th>Training Delivery Mode</th><th>Theory (Hours)</th><th>Practical (Hours)</th><th>OJT (Hours)</th><th>Total (Hours)</th></tr><tr><td>Classroom (offline)</td><td>25</td><td>20</td><td>00</td><td>45</td></tr><tr><td>Online</td><td>25</td><td>20</td><td>00</td><td>45</td></tr></table>(Refer Blended Learning Annexure for details)</td></tr>
<tr><td>12.</td><td>Assessment Criteria</td><td><table><tr><th>Theory (Marks)</th><th>Practical (Marks)</th><th>Project (Marks)</th><th>Viva (Marks)</th><th>Total (Marks)</th><th>Passing %age</th></tr><tr><td>30</td><td>70</td><td>-</td><td>-</td><td>100</td><td>50%</td></tr></table></td></tr>
<tr><td>13.</td><td>Is the NOS Amenable to Persons with Disability</td><td>☒ Yes ☐ No If “Yes”, specify applicable type of Disability: Visual, Hearing or Speech impairment, Locomotor Disability</td></tr>
<tr><td>14.</td><td>Progression Path After Attaining the Qualification, wherever applicable (Please show Professional and Academic progression)</td><td>After completing this program, participants can take up entry-level roles in cybersecurity.</td></tr>
<tr><td>15.</td><td>How will participation of women be encouraged?</td><td>The Program is gender neutral, although to increase women's participation, organizations are keeping aside a few seats to encourage female candidates.</td></tr>
<tr><td>16.</td><td>Other Indian languages in which the Qualification & Model Curriculum are being submitted</td><td>Once approved, the qualification will be available in Hindi or other Indian Languages.</td></tr>
<tr><td>17.</td><td>Is similar NOS available on NQR-if yes, justification for this qualification</td><td>☐ Yes ☒ No URLs of similar Qualifications:</td></tr>
<tr><td>18.</td><td>Name and Contact Details Submitting / Awarding Body SPOC
(In case of CS or MS, provide details of both Lead AB & Supporting ABs)</td><td>Name: Namrata Kapur
Email: Standards@nasscom.in
Contact No.: 0120-4990111
Website: https://nasscom.in</td></tr>
</table>

19.	Final Approval Date by NSQC: 18/02/2025	20. Validity Duration:36 Months	21. Next Review Date: 18/02/2028

Section 2: 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 apprenticeships undertaken after regular graduation. **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) **Industry & training experience:** 4 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **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 NOS, details of Any Upskilling Required for Trainer**	NA

Section 3: Assessment Related

1.	**Assessor's Qualification and experience in 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 full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **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) **Industry & Training Experience:** 2 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **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) **Industry & Training Experience:** 4 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **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 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 4: Evidence of the Need for the Standalone NOS

Provide Annexure/Supporting documents name.

1.	Government /Industry initiatives/ requirement (Yes/No): Yes, Industry Initiative
2.	Number of Industry validations provided: *11*
3.	Estimated number of people to be trained: 500
4.	Evidence of Concurrence/Consultation with Line/State Departments (In case of regulated sectors): (Yes/No): Applied

	If “No”, why:

Section 5: 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:** Performance and 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:** Acronym and Glossary *(Optional)*	Acronym and Glossary
7.	**Annexure/Supporting Document:** Standalone NOS-Performance Criteria Details Annexure/Document with PC-wise detailing as per NOS format (Mandatory- Public view)	NOS_Foundation of Cybersecurity
8.	**Supporting Document:** Model Curriculum *(Mandatory – Public view)*	MC_Foundation of Cybersecurity

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	Document business processes and the major functionalities and specifications of cyber security. Processes involved in the testing of cyber threats. Processes involved in managing the security configuration of networks and applications. Gather requirements for risk assessment and security audit tests	The individual in this role must work in a constantly changing environment where he/she needs to maintain secure networks and application systems while actively engaging with other stakeholders within the company to create streamlined operations. To perform his/her role and to collaborate with other stakeholders effectively, the individual requires a basic understanding of cyber security and different types of network devices	4.5
Professional and Technical Skills/ Expertise/ Professional Knowledge	Different types of Cyber Security Attacks and their applications (such DDoS/DoS attack, SQL injection attack, Phishing, Eavesdropping attack etc.) Different types of networks (such as Local Area Network (LAN), Wide Area Network (WAN), Virtual Private Network (VPN) etc.) Basic concepts of risk assessment and security audit tests and different security testing tools Different types of security controls	The individual in the role must have a basic knowledge across the different cyber-attacks and importance of cyber security measures This knowledge across various disciplines must be accompanied by an overall understanding of each discipline to perform this role effectively.	4.5

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
Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	Understanding of malwares such as Worms, Viruses, Trojan Horse, rootkits, Ransomware, Spyware, Adware, Logic Bombs etc. Basics of network models such as OSI (Open System Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol) Security risks and threats associated with applications and networks. Understanding and managing Identity and Access Management tools for User Identification, Authentication and Authorization Knowledge of Ethical Hacking and its applications Basics of incident management and incident response	The role demands a skill set that allows the individual to monitor cyber threats. This requires a wide range of skills. The individual, therefore, needs to have a good understanding of network devices, incident management, and security operations.	4.5
Broad Learning Outcomes/Core Skill	Knowledge of CIA (Confidentiality, Integrity and Availability) guiding principles for Information Security Basic knowledge of key networking terminologies (such as MAC Address, IP Address, DNS (Domain Name System) etc.)	The individual must apply his/her security monitoring skills along with a sound understanding of Identity and Access Management. This would enable him/her to better understand security control measures.	4.5

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
	How to check vulnerabilities and perform risk assessment Understanding of network monitoring processes How to prevent loss of data or data breaches		
Responsibility	Development of knowledge, skills, and competences Build and maintain relationships with colleagues and other teams Convince others to take appropriate action in different situations Manage and collaborate with stakeholders for project success	The role demands to work in a team to empower a culture of safety, security, and compliance in all aspects of cyber security activities and assist to deploy, monitor, audit, document, and maintain the life cycles of cyber security.	4.5

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	-	1 Unit per Trainee
2	Namp	Network scanning tool	Installed/Access to each PC/Laptop

3	Wireshark	Network Protocol analyzer	Installed/Access to each PC/Laptop
4	OWASP ZAP	Web application security Scanner	Installed/Access to each PC/Laptop
5	FreeIPA	Integrated security information management solution	Installed/Access to each PC/Laptop
6	OSSEC	Host-based intrusion detection system	Installed/Access to each PC/Laptop
7	Snort	Network intrusion detection and prevention system	Installed/Access to each PC/Laptop

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

S. No	Organization Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID	LinkedIn Profile
1	Skillsda	Kottaram Ramesh	Director-Engineering		9500123029	ram@skillsda.com	https://www.linkedin.com/in/kottaram-v-ramesh/
2	Fujitsu Consulting India Private Limited	Amitkumar Shrivastava	Global Fujitsu Distinguished Engineer (AI) & Fujitsu Fellow		8698132444	amitkumar.shrivastava@fujitsu.com / amit.ai.mldl@gmail.com	https://www.linkedin.com/in/amitkumar-shrivastava
3	Zoho	Abdul Rahim	Cybersecurity Analyst		7339471256	mailtorahim17@gmail.com	
4	Government Arts and Science College	Rithesh Adith	Assistant Programmer		9626592302	ritheshadith0@gmail.com	-
5	TCS	Sree Karthikeyan	Cybersecurity IAM Analyst		9626165768	sreekarthikeyan0898@gmail.com	https://www.linkedin.com/in/sree-karthikeyan-a88a84187/
6	Accolite Digital	Ayushmaan Pandey	Senior Software Engineer		8077386365	ayushmaan.pandey@accolitedigital.com	https://www.linkedin.com/in/ayushmaanpandey

7	Draup	MD Mahabub Alam	Architect		9731517171	mahabubalam@draup.com	https://www.linkedin.com/in/mdmahabubalam/
8	BBSSL	Sanjay Ramesh Babau	Senior software engineer		8438175943	sanjayrameshbabu.97@gmail.com	https://www.linkedin.com/in/sanjay-rameshbabu
9	CTS	Sivaranjani	Networking		8344016363	sivaranjaninallasamy97@gmail.com	
10	TCS	Vimal S	Cybersecurity IAM Analyst		8760861333	vimalvj333@gmail.com	
11	iAccept Softwares Pvt Ltd	B Mohan Kumar	Founder		9845208784	mohan@iaccept.in	https://www.linkedin.com/in/bmohankumar/

Annexure: Training Details

Training Projections:

Year	Estimated Training # of Total Candidates	Estimated training # of Women	Estimated training # of People with Disability
2025	500	-	-
2026	500	-	-
2027	500	-	-

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

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 NOS	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: Standalone NOS- Performance Criteria details

1. **Description:** This NOS describes the fundamentals of cybersecurity.

2. **Scope:**

The scope covers the following:

- Cybersecurity fundamentals.

3. **Elements and Performance Criteria**

PC 1. Understand Fundamentals of cybersecurity
PC2. Understanding Fundamentals of Networking
PC3. Gain knowledge of Basics of Security testing
PC4. Understanding Fundamentals of Access Management
PC5. Gain understanding of Fundamentals of Incident Management and Response
PC6. Understand Fundamentals of security operations

4. **Knowledge and Understanding (KU):**

KA1. Organizational policies and procedures for sharing data.
KA2. Organizational policies and procedures for documentation
KA3. Popular Cybersecurity Tools/Software/platforms and difference in their functionalities
KA4. Basic Understanding of information technology.

5. Generic Skills (GS):

GS1. Work independently and collaboratively.
GS2. Communicate with others in writing.
GS3. Ability to understand business impact and disseminate relevant information to others.
GS4. Check the work is complete and free from errors.
GS5. Apply balanced judgments to different situations.

Annexure: Assessment Criteria

Detailed PC-wise assessment criteria and assessment marks for the NOS are as follows:

S. No.	Assessment Criteria for Performance Criteria	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC 1.	Understand Fundamentals of cybersecurity	5	-	-	-
PC 2.	Understanding Fundamentals of Networking	5	14	-	-
PC 3.	Gain knowledge of Basics of Security testing	5	14	-	-
PC 4.	Understanding Fundamentals of Access Management	5	14	-	-
PC 5.	Gain understanding of Fundamentals of Incident Management and Response	5	14	-	-
PC 6.	Understand Fundamentals of security operations	5	14	-	-
Total Marks		**30**	**70**	**-**	**-**

Annexure: Assessment Strategy

Assessment System 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

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 on the basis of their main economic function, product, service or technology.