QUALIFICATION FILE

Analyst End Point Security

☒ 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: 5.5

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

1.	**Qualification Name**	**Analyst endpoint security**	
2.	**Sector/s**	**IT/ITeS**	
3.	**Type of Qualification: ☐ New ☒ Revised ☐ Has Electives/Options ☐ OEM**	**NQR Code & version of the existing /previous qualification:***QG-06-IT-01557-2023-V1.1-NASSCOM & Version 3*	**Qualification Name of the existing/previous version: Analyst endpoint security**
4.	**a. OEM Name** **b. Qualification Name** *(Wherever applicable)*	***Analyst endpoint security***	
5.	**National Qualification Register (NQR) Code &Version** (*Will be issued after NSQC approval*)	***QG-5.5-IT-045992025-V2-NASSCOM & Version 4***	**6. NCrF/NSQF Level: 5.5**
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 Endpoint Security Analyst is responsible for implementing and managing security measures for an organization's endpoint devices and data. This role involves installing and configuring endpoint security tools, monitoring security incidents, and enforcing security policies to ensure compliance with regulations.Key responsibilities include conducting audits of cloud environments, leveraging IT analytics for security reports, and utilizing AI-driven tools for anomaly detection. The analyst manages mobile devices through Mobile Device Management (MDM) solutions and applies data encryption strategies to protect sensitive information.Additionally, the analyst troubleshoots security issues, implements automated responses to incidents, and collaborates with cross-functional teams to communicate findings and recommend improvements. Overall, the Endpoint Security Analyst plays a vital role in identifying vulnerabilities and enhancing the organization's cybersecurity posture.	

<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:
*Relevant Experience in job roles related in IT/Computer Science/Cybersecurity.
The relevant experience would include work, internship, and apprenticeship after completing relevant educational qualifications

** UG or diploma with courses related to Engg./ Science

<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 3 Year UG**</td><td>-</td></tr>
<tr><td>2</td><td>Completed 3-Year Diploma** after 10th</td><td>3 years of relevant experience*</td></tr>
<tr><td>3</td><td>Previous Relevant qualification of NSQF level 5</td><td>1.5 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>18 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

<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>264</td><td>186</td><td>90</td><td>-</td><td>540</td></tr>
<tr><td>Online</td><td>264</td><td>186</td><td>90</td><td>-</td><td>540</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: **Professional progression**: Access to related qualification(s) at the next NSQF level – Senior Analyst-Endpoint Security, Senior Analyst- Application security, Senior Security Analyst, Senior- Security Operations Centre, Senior Cloud Security Analyst, etc. **Academic progression**: Access to other qualifications at the same NSQF level - Security Analyst, Analyst Endpoint Security, Analyst Security Operations Centre, Cloud Security Analyst, 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** **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's participation, organisations 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 Kapoor** **Email: Standards@nasscom.in** **Contact No.: 0120-4990111** **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.	Conduct the end-point security monitoring & response	SSC/N0912, V3.0	Core	5.5	06	80:00	70:00	30:00	00:00	180:00	30	50	-	20	100	30
2.	Carryout the Endpoint Security Management and Policy Enforcement	SSC/N0913, V3.0	Core	5.5	05	85:00	35:00	30:00	00:00	150:00	30	50	-	20	100	30
3.	Carryout the Installation and Infrastructure Support for Endpoint Security	SSC/N0965, V1.0	Core	5.5	05	75:00	45:00	30:00	00:00	150:00	30	50	-	20	100	30
4.	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					**18**	**264:00**	**186:00**	**90:00**	**00:00**	**540:00**	**110**	**180**	**-**	**60**	**350**	**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 **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 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) **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, 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 the Qualification

Provide Annexure/Supporting documents name.

1.	Latest Skill Gap study (not older than 2 years) (Yes/No):
2.	Latest Market Research Reports or any other source (not older than 2 years) (Yes/No):
3.	Government/Industry initiatives/requirement (Yes/No):
4.	Number of industry validations provided:21
5.	Estimated number of people to be trained and employed:
6.	Evidence of Concurrence/Consultation with Line/State Departments: 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_Q0905_Analyst end point 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	• Basic cyber security concepts • Common application/system vulnerabilities, threat actors and mitigations • Computer security incident detection & response activities	The job role involves a well-developed understanding of endpoint security concepts as can be seen from some of the requirements of the job role given in the adjacent cell. It covers IT related concepts	5.5

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
	• principles of intrusion detection, intrusion prevention, firewall operations, and other general security practices • general information about infrastructure security tools such as firewalls, network security monitoring, anti-malware, content management, OS hardening, email security, etc. • network threat prevention technologies such as firewall technologies and intrusion prevention • database and web server concepts • the features and functions in the endpoint security tool console and menus • common endpoint security support tools currently available • the importance of documenting, classifying, prioritizing service requests received over voice calls, email or internet and incident reports • the basic functionalities of the applications, hardware and/or access rights that the customers use • types of addresses used on networks and why they are used • Knowledge of Operating System Internals • ITIL framework knowledge • Mobile device management and mobile application management • obtain reports and notifications from the endpoint security tool and respond as per laid out process for the same • upgrade and maintain the endpoint security environment and clients • use IT analytics to generate comprehensive reports from Endpoint Protection • report the results of the monitoring, ticket raising and ticket closure activities using standard documentation following organisational procedures	like networking, Operating system internals, knowledge of ITIL framework and software development. It also requires knowledge and understanding about endpoint infrastructure, their security requirements, etc. The skills cover monitoring, analysing, researching, co-ordinating and testing. This requires a range of cognitive and practical skills through the application of clear choice of procedures in a known context. The role requires the individual to work in a familiar and routine context, however as the cyber security landscape is evolving, he/she should also be aware of the endpoints (computers, laptops, mobiles, printers, etc.) that are continuously being upgraded. The role requires the induvial to constantly monitor these changes and identify vulnerabilities to be resolved.	

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
	• create a database containing settings, privileges, events and security policies as per specifications • create and manage administrator accounts in the Endpoint Security Manager Console • install and configure clients on the endpoint security manager tool • configure Endpoint security replication, load balancing, and failover as per instructions provided • configure and implement Endpoint Protection domains as per instructions provided • analyse the automated scheduled scan reports and take remedial action • use reports and logs to identify security problems and monitor status and security events • interpret the results of reports and determine the priorities and actions to take to remediate the situation • monitor and troubleshoot an endpoint security environment, its security management tools and client content delivery • troubleshoot and remediate a virus outbreak or client installation failures • enable debugging and gather logs for technical support use • manage and apply policies such as virus and spyware protection policies, firewall policies, intrusion prevention policies, application and device control policies, update policies, and centralized exception policies		
Professional and Technical Skills/ Expertise/ Professional Knowledge	• basic cyber security concepts • common application/system vulnerabilities, threat actors and mitigations • computer security incident detection & response activities	As indicated by some of the knowledge and understanding requirements mentioned in the adjacent cell the job role holder need to have knowledge of general	5.5

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
	• principles of intrusion detection, intrusion prevention, firewall operations, and other general security practices • general information about infrastructure security tools such as firewalls, network security monitoring, anti-malware, content management, OS hardening, email security, etc. • network threat prevention technologies such as firewall technologies and intrusion prevention • database and web server concepts • the features and functions in the endpoint security tool console and menus • common endpoint security support tools currently available • the importance of documenting, classifying, prioritizing service requests received over voice calls, email or internet and incident reports • the basic functionalities of the applications, hardware and/or access rights that are used by the customers • types of addresses used on networks and why they are used • Knowledge of Operating System Internals • ITIL framework knowledge • Mobile device management and mobile application management	concepts and factual understanding in broad contexts of IT, Cyber security and endpoint devices (which include Desktops, Laptops, Mobile phones, Tablets, Printers, etc.) and their security components (Antivirus management, Antispyware, Desktop firewall, Device control, Email protection, Website browsing protection, Application control and network access control, Patch assessment and management, Access control and firewalls/Unified Threat Management devices, Intrusion Detection and Prevention systems, Remote Network Access, Endpoint DLP Endpoint Encryption). The job role also involves installing and configuring End Point Security (EPS) solutions as per instructions as well as troubleshooting and maintaining EPS solutions.	
Employment Readiness & Entrepreneurship **Skills & Mind-set/Professional Skill**	• Obtain reports and notifications from the endpoint security tool and respond as per laid out process for the same • use reports and logs to identify security problems and monitor status and security events • interpret the results of reports and determine the priorities and actions to take to remediate the situation • monitor and troubleshoot an endpoint security environment, its security management tools and client content delivery	As indicated by some of the performance criteria required of the job role holder, a range of cognitive and practical skills are required to identifying security problems using reports and logs, interpreting data, and prioritizing the application of solution based on the impact created. Also, the work requires the individual to employ analytical tools and information for problem solving.	5.5

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
	• monitor and troubleshoot protection and communication technologies using basic troubleshooting and other monitoring tools • troubleshoot and remediate a virus outbreak or client installation failures • enable debugging and gather logs for technical support use • use IT analytics to generate comprehensive reports from Endpoint Protection		
Broad Learning Outcomes/Core Skill	• use reports and logs to identify security problems and monitor status and security events • interpret the results of reports and determine the priorities and actions to take to remediate the situation • monitor and troubleshoot an endpoint security environment, its security management tools and client content delivery • monitor and troubleshoot protection and communication technologies using basic troubleshooting and other monitoring tools • troubleshoot and remediate a virus outbreak or client installation failures • enable debugging and gather logs for technical support use • use IT analytics to generate comprehensive reports from Endpoint Protection • Obtain reports and notifications from the endpoint security tool and respond as per laid out process for the same • report the results of the monitoring, ticket raising and ticket closure activities using standard documentation following organisational procedures • maintain a knowledge-base of the known problems and action taken for the same	The job role holder requires good understanding of endpoint security concepts and mathematical skill to perform the various evaluations, analysis and trend identification related activities required of the job. The job role holder also requires a good understanding of environment to understand the priorities of the business and threats in the environment. A large part of the work of the job role holders is collecting and organising information as indicated by the performance criteria in the adjacent cell as indicated by the performance criteria in the adjacent cell. The job role holder has to frequently communicate with stakeholders, staff, business users and specialists in the course of performing their job. They have to present reports, maintain databases,	5.5

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
	• create a database containing settings, privileges, events, and security policies as per specifications • verify the scope of endpoint assets and components to be monitored with authorised persons • collaborate with others to resolve information technology issues that are beyond own capabilities or job profile • btain help or advice from specialist if the problem is outside his/her area of competence or experience	etc. also as indicated by some of the performance criteria from the qualification given in the adjacent cell.	
Responsibility	• Troubleshoot and maintain endpoint security in an enterprise environment • comply with relevant legislation, standards, policies, and procedures	The Job role holder is responsible for the work of troubleshooting, maintaining, and implementing installing endpoint security. This work is done in a group; however each member of the group is fully responsible for their own work and learning and keeping the group updated.	5.5

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	-	
2	Antivirus and Anti-Malware	ClamAV	
3	Security Analytics and Reporting tool	ELK Stack	
4	Endpoint Detection and Response tool	Crowdstrike (Free trial version)	
5	Threat Intelligence Platforms	MISP (Malware Information Sharing Platform)	
6	Network and Data Encryption Tool	OpenSSL	
7	Cloud Integration Tool	Microsoft Azure (Free Tier)	
8	Configuration Management Tool	Ansible	
9	Incident Response and Forensic Tool	Wireshark	
10	Documentation and Reporting Software	Google Docs	
11	Vulnerability Assessment Tool	OpenVAS	

*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 the 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 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
SSC/N0912: Conduct the Endpoint Security Monitoring and Response	PC1. Verify the scope of endpoint assets and components to be monitored with authorized persons.	3	5	-	2
	PC2. Participate in security operations center shift schedules.	3	5	-	2
	PC3. Verify that endpoint security clients are online and functional.	3	5	-	2
	PC4. Obtain reports and notifications from endpoint security tools and respond per laid-out processes.	3	5	-	2
	PC5. Use reports and logs to identify security problems and monitor status and security events.	2	4	-	2
	PC6. Interpret the results of reports and determine priorities and actions to remediate situations.	2	4	-	2
	PC7. Respond to endpoint security client messages and apply solutions accordingly.	2	4	-	2
	PC8. Monitor and troubleshoot an endpoint security environment, its security management tools, and client content delivery.	2	3	-	1
	PC9. Monitor and troubleshoot protection and communication technologies using basic troubleshooting and other monitoring tools.	2	3	-	1
	PC10. Troubleshoot and remediate virus outbreaks or client installation failures.	2	3	-	1
	PC11. Use AI for anomaly detection to identify unusual patterns indicative of potential threats.	2	3	-	1
	PC12. Implement automated responses to neutralize threats in real-time.	2	3	-	1
	PC13. Integrate threat intelligence feeds to enhance monitoring capabilities and proactively address emerging threats.	2	3	-	1
	Total Marks	**30**	**50**	**-**	**20**
SSC/N0913: Carryout the Endpoint Security Management and Policy Enforcement	PC1. Enable debugging and gather logs for technical support use.	5	8	-	3
	PC2. Upgrade and maintain the endpoint security environment and clients.	5	7	-	3
	PC3. Manage and apply policies such as antivirus, spyware protection, firewall, and intrusion prevention.	4	7	-	3
	PC4. Use IT analytics to generate comprehensive reports from Endpoint Protection.	4	7	-	3
	PC5. Ensure compliance with relevant legislation, standards, policies, and procedures.	4	7	-	3
	PC6. Work within a zero-trust architecture, ensuring all access is authenticated and authorized.	4	7	-	3

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC7. Implement micro-segmentation to minimize lateral movement in case of a breach.	4	7	-	2
	Total Marks	**30**	**50**	**-**	**20**
SSC/N0965: Carryout the Installation and Infrastructure Support for Endpoint Security	PC1. Receive instructions for the installation of endpoint security tools.	5	8	-	3
	PC2. Create a database containing settings, privileges, events, and security policies.	5	7	-	3
	PC3. Configure clients for automatic updates and virus definition updates.	4	7	-	3
	PC4. Use Mobile Device Management (MDM) solutions for securing all mobile endpoints.	4	7	-	3
	PC5. Employ data encryption strategies to protect sensitive information at rest and in transit.	4	7	-	3
	PC6. Integrate endpoint security tools with cloud services to enhance visibility and protection.	4	7	-	3
	PC7. Conduct audits of cloud environments to ensure robust endpoint protection.	4	7		2
	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	-	-
	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		**110**	**180**	**-**	**60**

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.