QUALIFICATION FILE

Security Analyst

☒ 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

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>Qualification Name</td><td colspan="2">Security Analyst</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 ☐ Has Electives/Options ☐ OEM</td><td>NQR Code & version of the existing /previous qualification: 2021/ITES/ITSSC/04666 and Version 3</td><td>Qualification Name of the existing/previous version: Security Analyst</td></tr>
<tr><td>4.</td><td>Qualification Name (Wherever applicable)</td><td colspan="2">Security Analyst</td></tr>
<tr><td>5.</td><td>National Qualification Register (NQR) Code &Version
(Will be issued after NSQC approval)</td><td>QG-05-IT-03639-2025-V2-NASSCOM and Version 4</td><td>6. NCrF/NSQF Level: 5</td></tr>
<tr><td>7.</td><td>Award (Certificate/Diploma/Advance Diploma/ Any Other
(Wherever applicable specify multiple entry/exits also & provide details in annexure)</td><td colspan="2">Certificate</td></tr>
<tr><td>8.</td><td>Brief Description of the Qualification</td><td colspan="2">Individuals at this job are responsible for protecting organizational data by monitoring and analyzing threats, coordinating responses to information security incidents, managing and securing cloud environments, and executing phishing and social engineering defenses. They ensure robust security measures, mitigate risks, and maintain compliance with industry standards across digital platforms.</td></tr>
<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 2nd year of 3-year/ 4-year UG**</td><td>No experience required</td></tr>
</table>
</td></tr>
</table>

2.	Completed 3-Year Diploma** after 10th	1.5 year of relevant experience*
3.	Previous Relevant qualification of NSQF level 4	3 years of relevant experience*

10.	**Credits Assigned to this Qualification, Subject to Assessment** *(as per National Credit Framework (NCrF))*	16 Credits	**11. Common Cost Norm Category (I/II/III)** *(wherever applicable)***: II**
12.	**Any Licensing Requirements for Undertaking Training on This Qualification** *(wherever applicable)*	NA	
13.	**Training Duration by Modes of Training Delivery** *(Specify **Total Duration** as per selected training delivery modes and as per requirement of the qualification)*		

Training Delivery Mode	Theory (Hours)	Practical (Hours)	OJT (Mandatory) Hours	OJT (Recommended) Hours	Total (Hours)
Classroom (offline)	134:00	256:00	90:00	-	480:00
Online	134:00	256:00	90:00	-	480:00

☒ Offline Only ☒ Online Only ☐ Blended

(Refer Blended Learning Annexure for details)

14.	**Aligned to NCO/ISCO Code/s** *(if no code is available mention the same)*	NCO-2015/2522.0201
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: **Level 5: Security Analyst** **Level 6: Security Architect** **Level 7: SOC Specialist**
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**	
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** **Email: Standards@nasscom.in** **Contact No.: 0120-4990111** **Website: https://nasscom.in**	
23.	**Final Approval Date by NSQC: 18-02-2025**	**24. Validity Duration: 3 years**	**25. Next Review Date: 18-02-2028**

Section 2: Module Summary

NOS/s of Qualification

(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.	Monitor and Analyze Threats	SSC/N0954, V1.0	Core	5	5	40:00	80:00	30:00	00:00	150:00	30	50	-	20	100	22
2.	Coordinate with team and respond to Incidents	SSC/N0955, V1.0	Core	5	4	30:00	60:00	30:00	00:00	120:00	30	50	-	20	100	22
3.	Manage and Secure Cloud Data	SSC/N0956, V1.0	Core	5	3	20:00	40:00	30:00	00:00	90:00	30	50	-	20	100	22
4.	Execute Phishing and Social Engineering Defense	SSC/N0957, V1.0	Core	5	2	20:00	40:00	00:00	00:00	60:00	30	50	-	20	100	22
5.	Employability Skills (60 Hours)	DGT/VSQ/N0102, V1.0	Non-Core	4	2	24:00	36:00	00:00	00:00	60:00	20	30	-	-	50	12

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)
Duration (in Hours)/Total Marks					16	134:00	256:00	90:00	00:00	480:00	140	230	-	80	450	100

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 in any discipline, preferably Engineering/Science/Computer Science/Electronics and Engineering /Information Technology. **Industry & Training Experience:** 2 years of industry experience in the field of cyber security. **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 in any discipline, preferably Engineering/Science/Computer Science/Electronics and Engineering /Information Technology. **Industry & Training Experience:** 4 years of industry experience in field of cyber security.

		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 in any discipline, preferably Engineering/Science/Computer Science/Electronics and Engineering /Information Technology. **Industry & Training Experience:** 2 years of industry experience in the field of cyber security. **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 in any discipline, preferably Engineering/Science/Computer Science/Electronics and Engineering /Information Technology. **Industry & Training Experience:** 2 years of industry experience in the field of cyber security. **Certification: "Proctor"** 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 in any discipline, preferably Engineering/Science/Computer Science/Electronics and Engineering /Information Technology. **Industry & Training Experience:** 4 of industry experience in the field of cyber security. **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): 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): Yes
4.	Number of industry validations provided: 30
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_English_Q0901_Security Analyst_V3
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 cybersecurity concepts • Relevant networking concepts, protocols, and terminologies • Different types of threats, vulnerabilities, and attacks, including their impact on security	The job role of a Security Analyst at NSQF Level 5 requires a comprehensive understanding of cybersecurity principles and processes within a familiar context. This encompasses a range of IT-related concepts, including networking, data	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
	• Security frameworks, standards, and compliance requirements (e.g., ISO 27001, NIST) • Risk assessment methodologies and how they contribute to threat management • Techniques for incident detection, analysis, and response, including log analysis and digital forensics • Cloud security principles and best practices for securing cloud environments • Features, configurations, and specifications of cloud-based security solutions and applications • Procedures for coordinating and managing responses to information security incidents • Techniques for phishing and social engineering defense and how to implement awareness programs	management, and information systems, as well as a solid grounding in cybersecurity frameworks and protocols. The professional theoretical knowledge necessary for this role includes familiarity with security monitoring tools, threat detection methodologies, incident response strategies, and digital forensic techniques. Security Analysts must possess cognitive skills to assess security risks, analyze vulnerabilities, and implement appropriate mitigation strategies. Additionally, practical skills are essential for executing security measures and conducting thorough investigations of security incidents. This involves hands-on experience with various security technologies and the ability to apply established procedures in a known context. While the role typically involves routine tasks, the rapidly changing nature of cybersecurity threats necessitates continuous learning and adaptation. Security Analysts must remain vigilant and proactive, staying updated on emerging threats, new attack vectors, and innovative security solutions to effectively protect organizational assets.	
Professional and Technical Skills/ Expertise/ Professional Knowledge	• Fundamentals of cybersecurity and threat landscape • Different types of vulnerabilities and exposures in IT infrastructure	As indicated by some of the knowledge and understanding requirements mentioned in the adjacent cell, the job role holder needs to have knowledge of	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
	● Key aspects of threat detection, threat intelligence, and threat response techniques ● Various incident response methodologies and their stages ● Different types of security devices, firewalls, intrusion detection/prevention systems (IDS/IPS), and their configurations ● Security monitoring tools and systems, such as SIEM (Security Information and Event Management) ● Common issues and challenges in identifying, categorizing, and resolving security threats ● Best practices for log management, continuous monitoring, and network traffic analysis ● Key aspects of digital forensics and investigation procedures	specific cybersecurity principles and practices within a detailed context of information security management. He/she should be proficient in identifying vulnerabilities and threats in systems, implementing appropriate security measures, and analyzing security incidents. The individual must also understand various methodologies for risk assessment and mitigation, as well as be skilled in using security tools and technologies to monitor and protect information systems. Additionally, familiarity with compliance standards and regulations related to cybersecurity is essential for ensuring that the organization adheres to legal and ethical guidelines.	
Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	● Develop a proactive mindset to identify potential security vulnerabilities and take preventive action. ● Apply critical thinking skills to assess security threats and suggest mitigation strategies. ● Demonstrate problem-solving abilities in resolving information security incidents. ● Communicate effectively with team members and stakeholders about security risks and their potential impact on the organization. ● Plan and manage time efficiently to handle multiple security tasks and incidents simultaneously. ● Adapt to rapidly changing security environments and keep up-to-date with emerging threats and technologies.	As indicated by some of the performance criteria required of the job role holder, a range of cognitive and practical skills are necessary to effectively monitor and analyze security threats and incidents. This includes the ability to gather and interpret data related to information security, assess vulnerabilities, and implement preventive measures. Additionally, the role demands effective communication skills for coordinating incident response efforts, collaborating with team members, and engaging with stakeholders. Furthermore, the position emphasizes critical thinking and problem-solving skills to identify security trends and patterns,	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
	• Display entrepreneurial thinking to recommend innovative solutions for enhancing organizational security posture. • Leverage networking skills to collaborate with cybersecurity professionals and industry experts. • Utilize basic financial management skills to understand the cost implications of security measures and budget accordingly. • Exhibit resilience and stress management when dealing with high-pressure security incidents. • Drive self-motivation for continuous learning and skill development in the field of cybersecurity. • Show initiative in identifying areas for improvement in security processes and suggesting enhancements. • Apply leadership skills when coordinating small teams for incident response tasks or projects.	enabling the analyst to make informed decisions. An entrepreneurial mindset is also vital, as it fosters adaptability and innovation in developing security strategies and solutions. This blend of skills prepares the individual not only to fulfill their responsibilities in safeguarding information assets but also to contribute to the broader objectives of the organization, aligning with the NCrF/NSQF level descriptor that emphasizes job readiness and professional development.	
Broad Learning Outcomes/Core Skill	• Analyze security monitoring data to detect potential threats and vulnerabilities. • Identify the roles and responsibilities required in managing security operations and maintaining compliance. • Recognize the tools and techniques needed to configure, monitor, and troubleshoot security devices and systems. • Resolve technical issues related to security controls by following standard operating procedures and troubleshooting guidelines. • Maintain accurate records and logs of security-related activities, using standard documentation tools and templates. • Update the organization's security knowledge base with resolved incidents, investigations, and learned lessons. • Classify, record, and escalate security incidents according to severity and organizational protocols.	The job role holder requires a solid understanding of cybersecurity principles and practices to effectively identify and mitigate potential threats to information systems. This includes knowledge of various security technologies and tools, enabling the analyst to implement and manage security measures effectively. The job role holder also needs analytical skills to assess and interpret data related to security incidents and vulnerabilities. This involves evaluating logs, analyzing patterns, and identifying trends, which are critical for timely threat detection and response. The performance criteria emphasize the necessity for analytical proficiency to enhance decision-making processes.	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
	● Prepare concise and accurate reports on security incidents using predefined reporting formats and tools.	A significant part of the work involves collaboration and communication with various stakeholders, including IT teams, management, and external partners. The job role holder must articulate security risks, present findings, and recommend solutions clearly and effectively. This aspect is highlighted in the performance criteria, which focus on the importance of communication in fostering a secure organizational environment. Additionally, the job role requires the ability to maintain up-to-date knowledge of evolving cybersecurity threats and technologies, underscoring the need for continuous learning and adaptation. This reflects the core skills required for success in the role, as indicated by the learning outcomes associated with NSQF Level 5.	
Responsibility	● Perform continuous monitoring of network and system activities to identify security risks and anomalies. ● Analyze security alerts and events in real-time, providing timely and accurate incident reports. ● Ensure proper documentation of security incidents, investigations, and solutions in line with organizational policies. ● Prioritize and escalate critical incidents according to organizational guidelines and severity of the threat. ● Follow established protocols for incident response, coordinating with relevant teams to contain and mitigate security breaches. ● Obtain assistance from senior security experts when faced with complex security incidents or unresolved threats.	The job role holder is responsible for implementing and managing security measures to protect information and information systems from various cyber threats. This includes conducting threat analysis, monitoring security alerts, and responding to incidents. He/she is accountable for their own work and continuous learning in the field of information security and plays a supportive role in guiding less experienced team members. Additionally, the role involves collaborating with other stakeholders to ensure compliance with security policies and practices,	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
	• Stay updated with the latest cybersecurity tools, practices, and regulatory requirements in information security. • Implement changes in security configurations and policies as per organizational updates and emerging threats.	contributing to the overall security posture of the organization.	

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	With Wifi (2MBPS Dedicated)	
2	Relevant Software	• Cloud Security: OpenStack, CloudStack • Network Security and Monitoring: Wireshark • Security Information and Event Management (SIEM): Graylog • Endpoint Security: Wazuh • Programming languages such as Python, C/C++, Java, Ruby, etc. • Operating Systems like Linux, Windows	

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	Capital Numbers Infotech Private Limited	Paromita Biswas Panja	Executive Director	Unit No 8E4, 8th floor, EAST TOWER, MANI CASADONA IT BUILDING, Plot #2 F/4, AA II, F, Newtown, Kolkata, Chakpachuria, West Bengal 700156	033-67992222	info@capitalnumbers.com	-
2	Senrysa Technologies	Triparna Mukherjee	HR Business Partner & Leadership Acquisition	6th Floor, TOWER-1, GODREJ WATERSIDE, DP Block, Sector V, Bidhannagar, Kolkata, West Bengal 700091	033-66212222	mail@senrysa.com	-
3	DreamzTech Solutions	Kausiki Mazumder	Vice President Global Security	6th Floor, Ambient Building, AQ-7, near Techno Polis, AQ Block, Sector V, Bidhannagar, West Bengal 700091	033-4004062	-	-
4	TeckValley India Pvt. Ltd.	Chandrika Prasad	Assistant Manager- HR Recruitment	J-38, Block J, Sector 63, Noida, Uttar Pradesh 201301	0120-4631841/42	hr@teckvalley.com	-
5	RJ Software	S. Dutta	-	5 B, Sarat Bose Rd, Sreepally, Bhowanipore, Kolkata, West Bengal 700020	-	-	-
6	axiusSoftware	Jayanta Nandi	CEO		9831044315	sales@axiussoftware.com	-
7	intersoft	David Rakshit	CEO	Module #129, Salt Lake Electronics Complex, SDF Building, GP Block, Sector V, Bidhannagar, Kolkata, West Bengal 700091	90007332226		-
8	Codomotive Software	Abhishek Roy Chowdhury	CEO	-	-	ashok@qostechnology.in	-

9	FusionCharts	Mrindranil Goswami	Head of IT Operations	-	-	hello@fusioncharts.com	-
10	Tech Star Group	M.Mahadevan	Business Head Global	9th floor, Dallas Centre, Raidurg, Serilingampalle (M), Telangana 500032	-	infor@techstar.com	-
11	Socielo	Anghsuman Chakraborty	CEO & Founder	87E, 1, Selimpur Rd, Dhakuria, Naskar Para, Garfa, Kolkata, West Bengal 700031	9038584112	-	-
12	Kovair	Shibaji Gupta	CEO	6th Floor, PTI Building, DP Block, Sector V, Bidhannagar, Kolkata, West Bengal 700091	-	admin@kovair.com	-
13	Experis IT	Vamsi Krishna	Global Head	Plot J3, GP Block, Sector V, Bidhannagar, Kolkata, West Bengal 700091	-	finance@in.experis.com	-
14	ARB Software	Senjuli Roy	HR Head	-	-	info@arbsoft.com	-
15	Dgtalists Solutions Pvt. Ltd.	Sujay Saha	Founder	-	8910435874	info@dgtalists.com	-
16	Inspira Software Services Pvt. Ltd.	Neeloptal Bhattacharya	CEO	Webel IT Park, Rajarhat	-	support@inspirasw.com	-
17	Lee & Nee	Vikash Singh	CEO	-	-	accounts@lnsel.net	-
18	Hashcash	Raj Chowdhury	CEO	-	-	contact@hashcashconsultants.com	-
19	LabVantage	Rakesh Panda	CEO	-	-	company@tcgls.com	-
20	Sentient Geeks	Satyandra Hari	CEO	Webel IT Park, Rajarhat	-	MD@sentientgeeks.com	-
21	Sonata	Sanjay Guha	Group Head Business	Bangalore	-	info@sonata-software.com	-
22	Anntech	Debasmita Mukherjee	HR Head	D/2 Baghajatin, Kolkata- 700032	7980815656	info@anatech.in	-

23	Somnetics	Paromita Basu	Co Director	-	-	itservices@sonmeticservices.in	-
24	MaxMobility	Arijeet Mukherjee	CEO	-	-	info@maxmibility.com	-
25	Web Spinders Group	Chandan Chakraborty	Group Head	-	-	-	-
26	Konnectogrow	Shivangi Pandey	Director	#15A, 4th Floor, City Vista Suite No.511, Fountain Road, Kharadi, Pune, Maharashtra 411014	9325031747	share@konnectgrow.com	-
27	Outright Solution	Swati Agarwalla	HR Head	Godrej Genesis Building, 1505 Plot, Street Number 11, EP Block, Sector V, Bidhannagar, Kolkata, West Bengal 700091	-	-	-
28	NimbleTech	Dipanjan Mandal	Director	-	-	inquiry.nimbletech@gmail.com	-
29	Global Digital Care Group	Sudip Roy	Co Director	EC- 48 Ghosh Para, P.O.- Desh Bandhunagar, P.S.- Rajarhat, 24 PGS-N, Kolkata, West Bengal-700059	-	-	-
30	Merce Technologies	Jayant Bhatt	Operation Head	301 Technocity, X-5/3, T.T.C. Industrial Area, MIDC Industrial Area, Mahape, Navi Mumbai, Maharashtra 400710	-	accounts@remiges.tech	-

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
	500-1000	**400-800**	**250-500**	**150-300**		

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: **PMKVY**

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	• Handbooks • PowerPoint presentations slides • Reference material (books, online articles, websites, etc.)	
2	☒Imparting Soft Skills, Life Skills, and Employability Skills / Mentorship to Learners	• Video conferencing and collaboration tools	
3	☒Showing Practical Demonstrations to the learners		
4	☒Imparting Practical Hands-on Skills/ Lab Work/ workshop/ shop floor training	• Video Play presentations	

		• Design tools (Open Source) • Version control and file management tools	
5	☒Tutorials/ Assignments/ Drill/ Practice	• MCQ based tests	
6	☒Proctored Monitoring/ Assessment/ Evaluation/ Examinations		
7	☐On the Job Training (OJT)/ Project Work Internship/ Apprenticeship Training		

Annexure: Detailed Assessment Criteria

Proctored Online Assessments case study based questions also included in the assessment

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/N0954: Monitor and Analyze Threats	PC 1. monitor security alerts from firewalls, IDS, SIEM, and other security platforms continuously, ensuring immediate identification of potential threats	2	3	-	1
	PC 2. perform real-time analysis of security alerts, correlating them with system data to detect suspicious activities	1	3	-	1
	PC 3. ensure alerts are cross-verified with other logs (e.g., network, application) to confirm the legitimacy of the threat	1	3	-	1
	PC 4. categorize identified threats based on severity, impact on critical business operations, and sensitivity of data potentially compromised	2	2	-	1
	PC 5. utilize frameworks like MITRE ATT&CK to classify and understand the tactics, techniques, and procedures (TTPs) used in attacks	1	3	-	2
	PC 6. apply a risk-based approach to determine the urgency and priority of threat response	2	2	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 7. initiate incident investigations by collecting and preserving digital evidence from compromised systems, network devices, and endpoints following best practices	2	2	-	1
	PC 8. perform forensic analysis to reconstruct the sequence of events leading to a security breach or attempted attack	1	3	-	1
	PC 9. analyze collected data to pinpoint the root cause and identify attack vectors, aiding in understanding how the system was compromised	2	3	-	1
	PC 10. collaborate with the incident response team to isolate affected systems and mitigate ongoing threats	1	3	-	1
	PC 11. recommend remediation steps based on the investigation, including patching vulnerabilities, hardening systems, or improving security controls	1	3	-	1
	PC 12. use appropriate security tools (e.g., IDS, firewalls, SIEM) proficiently to detect, analyze, and respond to cyber threats	2	3	-	1
	PC 13. demonstrate knowledge of network protocols, system vulnerabilities, and attack vectors in the analysis and categorization of threats	1	2	-	1
	PC 14. analyze complex and voluminous data sets to identify patterns or anomalies indicative of potential security incidents	1	3	-	1
	PC 15. troubleshoot and resolve issues arising during the detection, analysis, and response phases of incident management	2	2	-	1
	PC 16. effectively communicate findings and analysis results to both technical and non-technical stakeholders	2	3	-	1
	PC 17. stay updated on emerging cyber threats, vulnerabilities, and security best practices, and apply this knowledge to improve monitoring and defense strategies	2	2	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 18. regularly update incident response and analysis techniques based on lessons learned from past incidents and evolving threat landscapes	2	3	-	1
	PC 19. document the analysis and findings in a detailed incident report for further action and knowledge sharing	2	2	-	1
	Total Marks	**30**	**50**	**0**	**20**
SSC/N0955: Coordinate with team and respond to Incidents	PC 1. establish and document clear escalation procedures for major security incidents, ensuring timely notification of Incident Response Team (IRT) and Threat Hunting Team	2	4	-	2
	PC 2. effectively communicate threat status, urgency, and required actions to relevant teams and management during an incident	2	4	-	1
	PC 3. isolate the compromised system	-	4	-	1
	PC 4. implement and configure SOAR tools to automate threat detection, investigation, and containment processes	2	4	-	2
	PC 5. refer to the organization's knowledge base to review past information security incidents and the methods used to handle them	3	5	-	2
	PC 6. allocate information security incidents to the relevant personnel for investigation and response	3	3	-	1
	PC 7. evaluate the severity and potential impact of identified threats, prioritizing them based on organizational risk and criticality	2	3	-	1
	PC 8. monitor the progress of investigations into information security incidents and escalate to the relevant personnel if the progress fails to meet established standards or service level agreements (SLAs)	2	3	-	2
	PC 9. conduct thorough post-incident investigations to determine the root cause of the security breach or attempted intrusion	2	3	-	2

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 10. provide input based on security trends and incident analysis to strengthen policy development and enforcement mechanisms	2	3	-	1
	PC 11. conduct regular vulnerability assessments to identify potential weaknesses in the organization's systems, networks, and applications	3	4	-	1
	PC 12. coordinate with IT teams to prioritize and apply security patches to address known vulnerabilities in a timely manner	2	4	-	1
	PC 13. effectively analyze complex data sets to detect patterns of suspicious activity or potential security breaches	3	2	-	2
	PC 14. adhere to the organization's policies, standards, procedures, guidelines, and service level agreements (SLAs) while coordinating responses to information security incidents	2	4	-	1
	Total Marks	**30**	**50**	**0**	**20**
SSC/N0956: Manage and Secure Cloud Data	PC 1. configure and manage threat protection, information protection, and identity protection features within the Microsoft 365 Defender Suite	1	3	-	1
	PC 2. deploy and manage Azure Security Center, Azure Firewall, and Azure Key Vault effectively	1	2	-	1
	PC 3. regularly review and update security configurations to address emerging threats and vulnerabilities	1	3	-	1
	PC 4. implement security measures across multiple cloud providers and servers	2	3	-	1
	PC 5. utilize SIEM tools and threat intelligence feeds to monitor cloud environments continuously	1	2	-	1
	PC 6. identify and report suspicious activities or anomalies within specified response times	1	3	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 7. investigate security incidents promptly and efficiently, documenting findings and remediation steps	2	2	-	1
	PC 8. implement corrective actions to mitigate the impact of incidents and prevent recurrence	1	2	-	-
	PC 9. manage user accounts, ensuring appropriate access based on roles and responsibilities	2	3	-	1
	PC 10. maintain records of user access changes and ensure timely de-provisioning of inactive accounts	2	3	-	1
	PC 11. implement and manage Multi-Factor Authentication (MFA) for all relevant user accounts, achieving a specified compliance rate	1	3	-	1
	PC 12. conduct regular access reviews, identifying and revoking unnecessary user permissions	1	2	-	1
	PC 13. identify and classify sensitive data types (e.g., PII, PHI) effectively within cloud environments	2	2	-	1
	PC 14. categorize data according to sensitivity levels and ensure appropriate protection measures are in place	1	2	-	1
	PC 15. implement and monitor DLP policies to prevent unauthorized data access and transmission	1	2	-	1
	PC 16. ensure adherence to industry regulations (e.g., GDPR, HIPAA, PCI DSS) by conducting regular audits and assessments	3	2	-	1
	PC 17. develop and deliver security awareness training programs for employees, achieving a specified participation rate	1	2	-	1
	PC 18. conduct regular vulnerability assessments on cloud environments, documenting findings and remediation efforts	1	2	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 19. ensure timely application of security patches and updates across all cloud services and applications	2	2	-	1
	PC 20. develop and implement backup procedures to ensure data integrity and availability	1	3	-	1
	PC 21. participate in disaster recovery drills, documenting lessons learned and updating recovery plans accordingly	2	2	-	1
	Total Marks	**30**	**50**	0	20
SSC/N0957: Execute Phishing and Social Engineering Defense	PC 1. employ advanced tools (e.g., Phishme) to analyze and assess the risk level of incoming emails	2	4	-	2
	PC 2. identify phishing attempts by examining emails for red flags such as suspicious sender addresses, urgent requests, and grammatical errors	2	4	-	2
	PC 3. conduct thorough risk assessments for potential phishing threats, factoring in data sensitivity and employee vulnerability	3	5	-	2
	PC 4. design and implement phishing simulation exercises to educate employees about phishing tactics	3	6	-	2
	PC 5. analyze employee responses to phishing simulations to identify knowledge gaps and areas needing improvement	3	4	-	1
	PC 6. employ digital forensics techniques to trace the origin of suspicious emails, utilizing IP addresses, DNS records, and metadata	3	4	-	1
	PC 7. investigate incidents of successful phishing attacks to assess damage and identify corrective actions to prevent recurrence	2	5	-	2
	PC 8. develop, implement, and update phishing prevention policies, ensuring compliance with industry standards and regulations	3	4	-	2

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 9. actively contribute to the development and maintenance of incident response plans related to phishing and social engineering attacks	2	4	-	1
	PC 10. ensure readiness for a coordinated response to phishing incidents, involving relevant stakeholders and utilizing established protocols	2	3	-	2
	PC 11. ensure compliance with data privacy and security regulations, conducting regular audits and assessments as necessary	2	3	-	2
	PC 12. prepare and present reports on phishing threat trends, employee training effectiveness, and incident response outcomes to management	3	4	-	1
	Total Marks	**30**	**50**	0	20
DGT/VSQ/N0102 Employability NOS for 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	-	-

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC12. Getting Ready for Apprenticeship & Jobs	2	3	-	-
	Total Marks	**20**	**30**	**-**	**-**
Grand Total Marks		**140**	**230**	**-**	**80**

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
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.