QUALIFICATION FILE

Security Operation Centre 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

1.	**Qualification Name**	**Security Operation Centre Analyst**	
2.	**Sector/s**	**IT/ITeS**	
3.	**Type of Qualification: ☐ New ☒ Revised ☐ Has Electives/Options ☐ OEM**	**NQR Code & version of the existing /previous qualification:** *2021/ITES/ITSSC/04668 and Version 3*	**Qualification Name of the existing/previous version: Analyst Security Operations Centre**
4.	**Qualification Name***(Wherever applicable)*	***Security Operation Centre Analyst***	
5.	**National Qualification Register (NQR) Code &Version** (*Will be issued after NSQC approval*)	*QG-05-IT-03638-2025-V2-NASSCOM & Version 4*	**6. NCrF/NSQF Level: 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 Analyst in the Security Operations Centre is responsible for detecting threats and monitoring events using Sysinternals tools. They analyze security events, respond to detected threats, and identify and mitigate cyber-attacks, ensuring robust protection of information systems while collaborating effectively within the security team.	
9.	**Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee**	**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	

S. No.	Academic/Skill Qualification (with Specialization - if applicable)	Required Experience (with Specialization - if applicable)
1.	Completed 2nd year of 3-year/ 4-year UG**	No experience required

		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)*	**☐ Offline Only ☐ Online Only ☒ Blended**

Training Delivery Mode	Theory (Hours)	Practical (Hours)	OJT (Mandatory) Hours	OJT (Recommended) Hours	Total (Hours)
Classroom (offline)	154:00	236:00	90:00	00:00	480:00
Online	154:00	236:00	90:00	00:00	480:00

(Refer Blended Learning Annexure for details)

14.	**Aligned to NCO/ISCO Code/s** *(if no code is available mention the same)*	NCO-2015/NIL
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: Analyst Security Operation Center** **Level 6: Security Incident Responder** **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.	Detect threats and monitor events using Sysinternal Tools	SSC/N0961, V1.0	Core	5	5	60:00	60:00	30:00	00:00	150:00	30	50	-	20	100	29
2.	Analize security events and response to detected threats	SSC/N0962, V1.0	Core	5	5	40:00	80:00	30:00	00:00	150:00	30	50	-	20	100	29
3.	Identify and response to cyber attack	SSC/N0963, V1.0	Core	5	4	30:00	60:00	30:00	00:00	120:00	30	50	-	20	100	29
4.	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	13
Duration (in Hours)/Total Marks					**16**	**154:00**	**236:00**	**90:00**	**00:00**	**480:00**	**110**	**180**	**-**	**60**	**350**	**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):

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: 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 ExitDetails*(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_Q0909_Analyst Security Operation Center
9.	**Supporting Document:** Career Progression *(Mandatory-Public View)*	Occupational Map-Cloud Computing
10.	**Supporting Document:** Occupational Map *(Mandatory)*	Occupational Map-Cloud Computing
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	• Fundamental cybersecurity principles and practices • Understanding of network architecture, protocols, devices, and terminology • Knowledge of cybersecurity incident detection, response, management, and recovery • Event and log analysis techniques, including packet analysis methodologies • Familiarity with cybersecurity frameworks and standards, such as NIST, ITIL, ISO/IEC 27001, and ISO/IEC 20000 • Awareness of operational procedures, including report generation, verification processes, and data correlation analysis • Understanding security vulnerabilities related to remote access technologies and associated attack patterns • Skills for conducting vulnerability assessments and identifying weaknesses in security infrastructure	The job role of an Analyst in a Security Operations Centre (SOC) demands a comprehensive understanding of cybersecurity concepts, including threat detection, incident response, and risk assessment. The analyst must possess knowledge of various security frameworks (such as NIST and ISO/IEC 27001), the principles of network security, and the methodologies for log analysis and event correlation. This understanding is essential for identifying vulnerabilities within the organizational infrastructure and effectively responding to security incidents, as indicated by the responsibilities associated with the job role.	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
	• Knowledge of data backup strategies, including types of backups (full, incremental) and recovery tools and methods • Comprehension of incident response protocols and incident handling methodologies • Understanding of defense-in-depth strategies to enhance organizational security posture • Ability to receive and analyze alarms and alerts from multiple enterprise sources to ascertain potential causes • Skill in interpreting and integrating data from diverse security tool sources • Competence in validating Intrusion Detection and Prevention System (IDPS) alerts through network traffic analysis • Capability to perform routine health checks on security solutions • Monitoring ICT systems' traffic and logs using various security technologies to detect threats and ensure system health	Skills required for this role encompass monitoring, analyzing, and investigating security incidents, along with coordinating responses to mitigate potential threats. Analysts must be proficient in using various security tools and technologies, which necessitates a combination of cognitive abilities and practical skills. This includes the ability to apply established procedures in familiar contexts while maintaining adaptability to rapidly changing cybersecurity scenarios. The role typically involves working in a structured environment with defined procedures; however, due to the dynamic nature of cybersecurity threats, individuals must remain alert and informed about emerging trends and techniques used by malicious actors. Continuous learning and professional development are essential to effectively counteract new security challenges and ensure the integrity of the organization's information systems.	
Professional and Technical Skills/ Expertise/ Professional Knowledge	• Fundamental cybersecurity principles and practices • Understanding of networking fundamentals, devices, and terminologies • Proficiency in cybersecurity incident detection, prevention, management, and response strategies • Expertise in event log analysis, packet analysis, and security monitoring techniques • Familiarity with security frameworks and standards such as NIST, ITIL, ISO/IEC 27001, and ISO/IEC 20000 • Operational competencies in report generation, validation, and incident documentation processes	As outlined in the adjacent cell, the job holder in the role of "Analyst Security Operation Centre" is expected to possess both factual and theoretical knowledge across various aspects of IT and cybersecurity. This includes a comprehensive understanding of security monitoring techniques, incident response strategies, and the analysis of logs, alarms, and alerts relevant to the field. The individual is responsible for continuously	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
	● Understanding of data analysis and correlation techniques to identify security anomalies ● Knowledge of security vulnerabilities related to remote access technologies and common attack patterns ● Skills in conducting vulnerability assessments and recognizing weaknesses in security systems ● Comprehension of data backup strategies, including full and incremental backups, and recovery methodologies	monitoring and analyzing the organization's network traffic and system logs to identify potential security threats. They are also tasked with responding to security alarms, managing incident response activities, and ensuring timely follow-up on ticket closure with clients. Furthermore, the role involves assessing and recommending enhancements to existing cybersecurity measures, ensuring compliance with organizational policies and security guidelines, and contributing to the overall security posture of the organization.	
Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	● Identify and gather relevant information to assess the security posture of critical systems and devices. ● Develop effective communication skills to articulate security concerns and incident responses to both technical and non-technical stakeholders. ● Collaborate with cross-functional teams to ensure comprehensive incident response and mitigation strategies. ● Demonstrate proactive problem-solving skills by addressing security incidents and identifying root causes to prevent recurrence. ● Exhibit adaptability and resilience in a fast-paced environment, managing stress and maintaining focus during security incidents. ● Cultivate a continuous learning mindset to stay updated on emerging cybersecurity threats, technologies, and best practices. ● Embrace entrepreneurial thinking by identifying opportunities for improving security processes and suggesting innovative solutions.	As indicated by the performance criteria required of the job role holder, the Analyst in the Security Operations Centre (SOC) is expected to possess a blend of cognitive and practical skills essential for effective employment readiness and entrepreneurship. These skills include the ability to analyze security incidents, evaluate potential threats, and respond promptly to emerging vulnerabilities. The job holder is also expected to demonstrate a proactive mindset by staying updated with the latest cybersecurity trends and best practices. Additionally, they must effectively communicate findings and collaborate with cross-functional teams, which enhances their adaptability and problem-solving capabilities within a dynamic work environment. This combination of skills fosters a professional	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
	● Apply time management skills to prioritize tasks effectively, ensuring timely responses to security incidents and alerts. ● Engage in networking and professional development activities to build relationships within the cybersecurity community. ● Foster teamwork and collaboration by sharing knowledge and insights with peers and mentoring junior analysts.	attitude towards continuous learning and innovation, aligning with the NCrF/NSQF level descriptor for Level 5.	
Broad Learning Outcomes/Core Skill	● Evaluate the severity of security incidents by analyzing various contextual factors, including potential impact and urgency. ● Establish the relationships between different security incidents and their interdependencies to understand the broader threat landscape. ● Manually review system and application logs to identify security vulnerabilities and suspicious activities. ● Identify root causes of security incidents by considering architectural contexts, exploitation methods, and likelihood of occurrence. ● Validate security alerts to differentiate between false positives and legitimate threats, ensuring accurate threat assessment. ● Analyze network traffic patterns to identify anomalies indicative of potential security breaches. ● Recognize trends and recurring issues in security data to enhance future threat detection capabilities. ● Perform event correlation across multiple data sources to enhance situational awareness and evaluate threat levels. ● Monitor organizational traffic and logs generated by ICT systems using security technologies to detect vulnerabilities and operational health. ● Track external threat intelligence from reputable sources (e.g., CERTs, security vendors) to stay informed about potential risks.	The job role holder requires a strong analytical mindset and critical thinking skills to effectively investigate security incidents and analyze patterns from data collected during threat monitoring. This involves evaluating potential risks and making informed decisions based on real-time data. The job role holder also needs a solid understanding of cybersecurity principles, including familiarity with various security tools and technologies. This knowledge enables them to identify vulnerabilities and propose appropriate mitigation strategies that align with organizational security policies. A significant aspect of the role involves the collection, organization, and interpretation of security data. The job holder must demonstrate the ability to compile and synthesize information from various sources to support threat analysis and incident response, as indicated by the performance criteria in the adjacent cell. Furthermore, the job role holder must possess strong communication skills to	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
	• Gather and assess security posture information for identified devices and systems to enhance overall security measures. • Collect logs from diverse ICT devices and applications as mandated by organizational security protocols.	collaborate effectively with colleagues and stakeholders. They are expected to prepare and present reports on security incidents, trends, and recommendations, while also maintaining clear documentation of processes and protocols as highlighted by the performance criteria provided in the adjacent cell.	
Responsibility	• Adhere to organizational protocols for incident investigation and resolution. • Participate in a 24/7 security operations center shift schedule, ensuring continuous monitoring. • Receive and review shift handover documentation, including relevant information and instructions for ongoing incidents. • Seek assistance or guidance from specialists for complex issues beyond personal expertise. • Maintain up-to-date knowledge of industry standards, security tools, and emerging threats to enhance operational effectiveness. • Document and report security incidents, providing accurate and detailed accounts for future reference. • Analyze alerts and incidents to identify potential security threats and vulnerabilities. • Collaborate with team members to develop and implement effective security measures and incident response strategies.	The job involves monitoring and analyzing security alerts, identifying potential security incidents, and responding to them in accordance with established protocols and policies. This role requires collaboration within a team, yet each analyst is responsible for their own work and professional development while ensuring timely communication of findings and updates to the group.	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	With Wifi (2MBPS Dedicated)	1 Unit per Trainee
2	Relevant Software	• Security Information and Event Management (SIEM): Graylog • Threat Intelligence Platforms (TIPs): ThreatConnect • EDR tools: Wazuh • Ticketing Tool: osTicket • Active Directory: FreeIPA • Operating Systems like Kali Linux, Parrot OS, Windows, macOS etc.	1 Unit per Trainee

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	Sonata	Sanjay Guha	Group Head Business	Bangalore	-		-
2	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,	033-67992222	info@capitalnumbers.com	NA

				Newtown, Kolkata, Chakpachuria, West Bengal 700156			
3	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	
4	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	-	
5	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	
6	RJ Software	S. Dutta	-	5 B, Sarat Bose Rd, Sreepally, Bhowanipore, Kolkata, West Bengal 700020	-	-	
7	axiusSoftware	Jayanta Nandi	CEO		9831044315	sales@axiussoftware.com	

8	intersoft	David Rakshit	CEO	Module #129, Salt Lake Electronics Complex, SDF Building, GP Block, Sector V, Bidhannagar, Kolkata, West Bengal 700091	90007332226		
9	Codomotive Software	Abhishek Roy Chowdhury	CEO	-	-	ashok@qostechnology.in	
10	FusionCharts	Mrindranil Goswami	Head of IT Operations	-	-	hello@fusioncharts.com	
11	Tech Star Group	M.Mahadevan	Business Head Global	9th floor, Dallas Centre, Raidurg, Serilingampalle (M), Telangana 500032	-	infor@techstar.com	
12	Socielo	Anghsuman Chakraborty	CEO & Founder	87E, 1, Selimpur Rd, Dhakuria, Naskar Para, Garfa, Kolkata, West Bengal 700031	9038584112	-	
13	Kovair	Shibaji Gupta	CEO	6th Floor, PTI Building, DP Block, Sector V, Bidhannagar, Kolkata, West Bengal 700091	-	admin@kovair.com	
14	Experis IT	Vamsi Krishna	Global Head	Plot J3, GP Block, Sector V,	-	finance@in.experis.com	

				Bidhannagar, Kolkata, West Bengal 700091			
15	ARB Software	Senjuli Roy	HR Head	-	-	info@arbsoft.com	
16	Dgtalists Solutions Pvt. Ltd.	Sujay Saha	Founder	-	8910435874	info@dgtalists.com	
17	Inspira Software Services Pvt. Ltd.	Neeloptal Bhattacharya	CEO	Webel IT Park, Rajarhat	-	support@inspirasw.com	-
18	Lee & Nee	Vikash Singh	CEO	-	-	accounts@lnsel.net	-
19	Hashcash	Raj Chowdhury	CEO	-	-	contact@hashcashconsultants.com	-
20	LabVantage	Rakesh Panda	CEO	-	-	company@tcgls.com	-
21	Sentient Geeks	Satyandra Hari	CEO	Webel IT Park, Rajarhat	-	MD@sentientgeeks.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	**400-750**	**200-400**	**100-200**		

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:

1. **English**
2. **Hindi**

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 assessment case study-based question 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/ SSC/N0961: Detect threats and monitor events using Sysinternal Tools	PC 1. confirm the range of information assets and system components to be monitored in collaboration with authorized personnel	1	2	-	1
	PC 2. employs designated monitoring and data collection techniques and tools in accordance with organizational procedures and policies	2	2	-	1
	PC 3. oversee the organization's traffic and logs generated by ICT systems using various security technologies to identify security threats and assess the health of the ICT systems	1	2	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 4. oversee external data sources such as Computer Network Defense (CND) vendor websites, Computer Emergency Response Teams, SANS, and Security Focus	1	2	-	-
	PC 5. identify security issues that could affect the enterprise	1	1	-	1
	PC 6. perform detailed email analysis to identify phishing attempts by reviewing suspicious elements such as email addresses, links, or domain names, ensuring alignment with legitimate sources	1	1	-	1
	PC 7. analyze unexpected attachments or links in emails to detect and prevent potential malware downloads, utilizing phishing detection techniques to safeguard the organization's network	1	1	-	1
	PC 8. verify sender authenticity by cross-checking the sender's email address against the organization it claims to represent, applying phishing analysis methods to prevent fraudulent emails from compromising security	1	1	-	-
	PC 9. use Sysinternals tools (such as Process Explorer, Autoruns, and TCPView) to identify and examine potential malware or suspicious processes on the network	1	2	-	1
	PC 10. utilize Sysinternal tools (such as Process Explorer, Autoruns, and TCPView) for thorough system investigations to detect unauthorized changes or applications that may impact security.	1	2	-	-
	PC 11. gather logs from all types of ICT systems, devices, and applications as mandated by the organization	1	2	-	-

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 12. maintain continuous monitoring of all critical infrastructure, including servers, cloud workloads, applications, and networks, to identify signs of intrusion or suspicious activity around the clock	1	2	-	-
	PC 13. employ SIEM (Security Information and Event Management) or XDR (Extended Detection and Response) tools to consolidate alerts, examine telemetry data, and identify threats in real-time	1	2	-	1
	PC 14. analyze trends and patterns utilizing the SIEM tool	1	2	-	-
	PC 15. collaborate with enterprise-wide Computer Network Defense (CND) teams to verify network alerts	1	2	-	1
	PC 16. conduct event correlation using collected information to enhance situational awareness and assess the potential threat level	1	2	-	1
	PC 17. conduct a thorough analysis of log data gathered from different network events to identify anomalies	2	2	-	1
	PC 18. recognize standard activities and detect anomalies that suggest suspicious behavior	1	2	-	1
	PC 19. support the identification of real cyber threats by filtering out false positives and classifying threats based on their severity to ensure prompt action	1	2	-	1
	PC 20. utilize AI-powered SIEM tools to enhance the precision of threat detection progressively.	1	2	-	1
	PC 21. prioritize the service request according to organizational procedures and policies	1	2	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 22. obtain help or advice from specialist if the problem is outside his/her area of competence or experience	1	2	-	1
	PC 23. report the results of the monitoring, ticket raising and ticket closure activities using standard documentation following organisational procedures	1	2	-	-
	PC 24. participate in 24/7 security operations centre shift schedule	1	2	-	1
	PC 25. receive shift handover along with relevant information, authorities and instructions	1	2	-	1
	PC 26. comply with relevant legislation, standards, policies and procedures	1	1	-	1
	PC 27. maintain a knowledge base of the known problems	1	2		-
	PC 28. use escalation matrix for unresolved tickets within agreed turnaround times	1	1		1
	Total Marks	**30**	**50**	**0**	**20**
SSC/N0962: Analyze security events and response to detected threats	PC 1. receive and evaluate alarms and alerts from multiple sources across the enterprise, identifying potential causes and determining the underlying issues behind the alerts	2	2	-	1
	PC 2. maintain up-to-date inventories of all IT assets, including applications, databases, servers, cloud services, and endpoints, to ensure comprehensive protection and security	1	2	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 3. utilize asset discovery tools (Cacti, IP Scanning, etc.) to monitor and track changes, identify vulnerabilities, and assess potential security risks within the IT infrastructure	1	2	-	1
	PC 4. regularly implement patches, upgrades, and updates for security tools, including firewalls, antivirus, and monitoring software, to ensure continuous protection and optimal functioning of the Security Operations Centre (SOC)	2	2	-	1
	PC 5. contribute to the development of backup policies and procedures, ensuring data availability and integrity to support business continuity and disaster recovery efforts	1	2	-	1
	PC 6. conduct vulnerability assessments to identify potential weaknesses across IT resources, ensuring comprehensive analysis and reporting to enhance the organization's security posture	1	2	-	1
	PC 7. determine which information assets and system components could be affected by identified security incidents	1	2	-	-
	PC 8. analyze detected malicious activities to assess exploited vulnerabilities, methods of exploitation, and their impact on systems and data	1	2	-	1
	PC 9. analyze log files from multiple sources to detect potential threats to network security	1	3	-	1
	PC 10. conduct triage for computer network defense (CND) incidents, which involves evaluating the scope, urgency, and potential impact of each incident	1	2	-	1
	PC 11. conduct and assist in penetration testing activities to simulate cyberattacks, identifying vulnerabilities and strengthening the organization's security posture	2	2	-	1
	PC 12. utilize a Security Information and Event Management (SIEM) tool to correlate and analyze events for the detection of IT security incidents	2	2	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 13. collect and secure evidence related to identified incidents	1	2	-	1
	PC 14. investigate the methods used to gain access to the compromised information assets and system components	2	3	-	1
	PC 15. mitigate various types of vulnerabilities and their corresponding attacks on the system	1	2	-	1
	PC 16. decide on the suitable response based on the identification and analysis of anomalous activity	1	2	-	1
	PC 17. provide suggestions for specific actions to address incidents	1	2	-	1
	PC 18. conduct a health assessment of the security solution	1	2	-	1
	PC 19. utilize external information resources for conducting incident investigations	1	2	-	-
	PC 20. notify the appropriate individuals about any incidents that cannot be resolved or mitigated, adhering to organizational procedures	1	2	-	1
	PC 21. adhere to organizational protocols for closing incidents	1	2	-	1
	PC 22. document and report incident management activities in accordance with organizational procedures and standard documentation practices	1	2	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 23. monitor and record incidents from the initial detection to the final resolution using a SIEM tool	2	2	-	-
	PC 24. incorporate the assets into the SIEM solution for log analysis	1	2	-	-
	Total Marks	**30**	**50**	**0**	**20**
SSC/N0963: Identify and response to cyber attack	PC 1. utilize advanced security tools (Wireshark, KisMAC, NetStumbler, etc.) to monitor network traffic, system logs, and user behavior continuously for signs of suspicious activity	3	4	-	1
	PC 2. leverage threat intelligence feeds to remain informed about emerging threats and attack patterns	2	3	-	1
	PC 3. employ Security Information and Event Management (SIEM) solutions to aggregate and correlate security events from multiple sources to identify potential incidents	2	4	-	2
	PC 4. apply algorithms for detecting deviations from normal behavior, including unusual network traffic or unauthorized access attempts	2	3	-	2
	PC 5. correlate alerts from various sources when suspicious activities are detected to determine potential incidents	2	4	-	2

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 6. categorize incidents based on severity, impact, and type (e.g., data breach, malware infection, denial-of-service attack)	3	3	-	1
	PC 7. take immediate containment measures, such as isolating affected systems or disabling compromised accounts	2	4	-	1
	PC 8. perform thorough investigations to understand the root cause of attacks, identify attacker methods, and assess damage extent	2	3	-	1
	PC 9. develop a detailed timeline of events to reconstruct the attack sequence	2	4	-	2
	PC 10. isolate affected systems or networks to prevent further spread of the attack	2	4	-	1
	PC 11. identify and remove malicious software from infected systems effectively	2	4	-	2
	PC 12. patch known vulnerabilities to prevent future attacks	2	3	-	2
	PC 13. use backup procedures to restore lost or corrupted data	2	4	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 14. document the incident response process for future reference	2	3	-	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	-	-
	PC12. Getting Ready for Apprenticeship & Jobs	2	3	-	-
	Total Marks	**20**	**30**	**-**	**-**
Grand Total Marks		**110**	**180**	**-**	**60**

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 what an individual performing that task should know and do.
Qualification	A formal outcome of an assessment and validation process is obtained when a the 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 about 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.