QUALIFICATION FILE

Analyst Application 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

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 1.5

<table>
<tr><td><b>1.</b></td><td><b>Qualification Name</b></td><td colspan="2"><b>Analyst Application Security</b></td></tr>
<tr><td><b>2.</b></td><td><b>Sector/s</b></td><td colspan="2"><b>IT/ITeS</b></td></tr>
<tr><td><b>3.</b></td><td><b>Type of Qualification:</b> ☐ <b>New</b> ☒ <b>Revised</b> ☐ <b>Has Electives/Options</b> ☐ <b>OEM</b></td><td><b>NQR Code & version of the previous qualification:</b> <i>2021/ITES/ITSSC/04667 and Version 3</i></td><td><b>Qualification Name of the existing/previous version: Analyst Application Security</b></td></tr>
<tr><td><b>4.</b></td><td><b>Qualification Name</b> <i>(Wherever applicable)</i></td><td colspan="2"><b><i>Analyst Application Security</i></b></td></tr>
<tr><td><b>5.</b></td><td><b>National Qualification Register (NQR) Code &Version</b>
(<i>Will be issued after NSQC approval</i>)</td><td><i>QG-05-IT-03637-2025-V2-NASSCOM and Version 4</i></td><td><b>6. NCrF/NSQF Level: 5</b></td></tr>
<tr><td><b>7.</b></td><td><b>Award (Certificate/Diploma/Advance Diploma/ Any Other</b> <i>(Wherever applicable specify multiple entry/exits also & provide details in annexure)</i></td><td colspan="2">Certificate</td></tr>
<tr><td><b>8.</b></td><td><b>Brief Description of the Qualification</b></td><td colspan="2">The job involves managing application security hardening and vulnerability assessments, accessing APIs to ensure secure integration, and overseeing the security of deployed applications and solutions. The role focuses on monitoring for potential breaches and compromises, implementing security measures, and maintaining robust defenses against evolving cybersecurity threats.</td></tr>
<tr><td><b>9.</b></td><td><b>Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee</b></td><td colspan="2">a. <b>Entry Qualification & Relevant Experience:</b>
*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>
<tr><td>2.</td><td>Completed 3-Year Diploma** after 10th</td><td>1.5 year of relevant experience*</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td></td><td colspan="2"><table><tr><td>3.</td><td>Previous Relevant qualification of NSQF level 4</td><td>3 years of relevant experience*</td></tr></table></td></tr>
<tr><td><b>10.</b></td><td><b>Credits Assigned to this Qualification, Subject to Assessment</b> <i>(as per National Credit Framework (NCrF))</i></td><td>17 Credits</td><td><b>11. Common Cost Norm Category (I/II/III)</b> <i>(wherever applicable)</i><b>: II</b></td></tr>
<tr><td><b>12.</b></td><td><b>Any Licensing Requirements for Undertaking Training on This Qualification</b> <i>(wherever applicable)</i></td><td colspan="2">NA</td></tr>
<tr><td><b>13.</b></td><td><b>Training Duration by Modes of Training Delivery</b> <i>(Specify <b>Total Duration</b> as per selected training delivery modes and as per requirement of the qualification)</i></td><td colspan="2"><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><b>Classroom (offline)</b></td><td>174:00</td><td>246:00</td><td>90:00</td><td>00:00</td><td>510:00</td></tr>
<tr><td><b>Online</b></td><td>174:00</td><td>246:00</td><td>90:00</td><td>00:00</td><td>510:00</td></tr>
</table>
<b>☒ Offline Only ☒ Online Only ☐ Blended</b>

<i>(Refer Blended Learning Annexure for details)</i></td></tr>
<tr><td><b>14.</b></td><td><b>Aligned to NCO/ISCO Code/s</b> <i>(if no code is available mention the same)</i></td><td colspan="2">NCO-2015/NIL</td></tr>
<tr><td><b>15.</b></td><td><b>Progression Path After Attaining the Qualification, wherever applicable</b> <i>(Please show Professional and Academic progression)</i></td><td colspan="2">This entry should refer to one or more of the following:
<b>Level 5: Analyst Application Security</b>
<b>Level 6: Security Architect</b>
<b>Level 7: System Security Manager</b></td></tr>
<tr><td><b>16.</b></td><td><b>Other Indian languages in which the Qualification & Model Curriculum are being submitted</b></td><td colspan="2">Hindi</td></tr>
<tr><td><b>17.</b></td><td><b>Is similar Qualification(s) available on NQR-if yes, justification for this qualification</b></td><td colspan="2"><b>☐ Yes ☒ No URLs of similar Qualifications:</b></td></tr>
</table>

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, organizations are keeping aside few seats to encourage the female candidates	
20.	**Are Greening/Environment Sustainability Aspects covered** (*Specify the NOS/Module which Covers it)*	**☐ Yes ☒ No**	
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.	Access API and application for security	SSC/N0958, V1.0	Core	5	05	50:00	70:00	30:00	00:00	150:00	30	50	-	20	100	28
2.	Manage application security, hardening and vulnerability	SSC/N0959, V1.0	Core	5	05	50:00	70:00	30:00	00:00	150:00	30	50	-	20	100	28
3.	Oversee the Cloud security of deployed applications and solutions to detect potential breaches and compromises	SSC/N0960, V1.0	Core	5	05	50:00	70:00	30:00	00:00	150:00	30	50	-	20	100	28
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	16
Duration (in Hours)/Total Marks					**17**	**174:00**	**246:00**	**90:00**	**00:00**	**510:00**	**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 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_Q0903_Analyst Application Security
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	● Fundamental cybersecurity principles ● Knowledge of secure Software Development Lifecycle (SDLC) ● Types of applications and their common security requirements ● Emerging technologies in application security ● Essentials of mobile and cloud application security ● Systems engineering theories, concepts, and methods ● Monitoring of Systems/Product Life Cycle ● Proficiency in scripting languages (Shell Script, JavaScript) ● Monitoring application health and security threats using Security Information and Event Management (SIEM) tools ● Establishment of operational processes for effective log management ● Collaboration with enterprise-wide Computer Network Defense (CND) teams to validate network alerts ● Research and application of best practices for hardening applications ● Identification of trends and patterns according to standard guidelines ● Collection of web-based information through automated tools and techniques	The job role of an Analyst in Application Security demands a comprehensive understanding of application security principles, as reflected in the requirements associated with the position. This includes a solid grasp of key concepts such as application development methodologies, application testing techniques, scripting languages, Security Information and Event Management (SIEM) systems, and broader cybersecurity frameworks. A deep technical knowledge of application security in various contexts is essential for effectively identifying and mitigating vulnerabilities. The skills required for this role encompass monitoring systems, analyzing data, conducting research, coordinating with teams, and executing rigorous testing protocols. These competencies necessitate a combination of cognitive and practical skills, enabling the analyst to choose appropriate procedures and approaches for various security challenges.	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
		While the role operates within familiar and routine contexts, it is crucial for the individual to remain alert to the rapidly evolving cyber threat landscape. Continuous vigilance regarding emerging attack vectors and system vulnerabilities is essential, as is the ability to implement timely interventions to safeguard applications and systems.	
Professional and Technical Skills/ Expertise/ Professional Knowledge	● Basic concepts of cyber security and information security principles ● In-depth understanding of the secure Software Development Lifecycle (SDLC) ● Knowledge of different types of applications and their common security requirements ● Awareness of new technological advancements in application security ● Fundamentals of mobile and cloud application security practices ● Familiarity with systems engineering theories, concepts, and methods throughout the Systems/Product Life Cycle ● Proficiency in scripting languages (e.g., Shell Script, JavaScript)	As indicated by the knowledge and understanding requirements outlined in the adjacent cell, the job role holder needs to possess a comprehensive understanding of both factual and theoretical concepts related to IT, Cybersecurity, and various application environments (including computer, mobile, and cloud). This position requires proficiency in the processes and procedures for conducting vulnerability assessments on applications, performing source code reviews, and executing tests on the source code. The individual should also be adept at suggesting remediation actions, implementing hardening measures, and monitoring threats in accordance with established security policies. A thorough understanding of security frameworks, compliance requirements, and risk management practices is vital to effectively mitigate security risks associated with applications.	5

NCrF/NSQF Level Descriptors	Key requirements of the job role/ outcome of the qualification	How the job role/ outcomes relate to the NCrF/NSQF level descriptor	NCrF/NSQF Level
Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	● Demonstrate adaptability to changing technologies and methodologies in application security. ● Communicate effectively with technical and non-technical stakeholders to convey security issues and solutions. ● Collaborate with cross-functional teams to integrate security practices within application development processes. ● Apply critical thinking to assess risks and devise appropriate mitigation strategies. ● Maintain a proactive approach to learning about emerging threats and security technologies. ● Exhibit problem-solving skills to diagnose and resolve security-related issues in applications. ● Cultivate an entrepreneurial mindset to identify opportunities for improving security measures and processes. ● Develop project management skills to prioritize tasks and manage timelines for security assessments. ● Engage in continuous professional development to stay updated on industry standards and best practices. ● Foster a culture of security awareness within the organization by educating team members on security protocols and practices.	As indicated by the performance criteria required of the job role holder, a diverse set of cognitive and practical skills is essential for effectively gathering information, researching, and analyzing security frameworks. The role demands the ability to identify vulnerabilities, trends, and patterns through various methodologies and tools. Furthermore, the job holder must demonstrate a proactive approach to problem-solving and adaptability, allowing them to respond swiftly to emerging security threats.	5
Broad Learning Outcomes/Core Skill	● Evaluate the significance of application security risks by considering various contextual factors. ● Conduct manual source code reviews to identify security vulnerabilities. ● Isolate the root causes of vulnerabilities and propose fixes, incorporating details such as architectural structure, exploitation techniques, and likelihood of exposure.	The job role holder requires a solid understanding of application security principles and analytical skills to perform various evaluations, analyses, and trend identification activities pertinent to the position. A significant aspect of the role involves collecting, organizing, and	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
	● Validate data to differentiate between false positives and actual vulnerabilities. ● Analyze application traffic to detect anomalous behavior and potential threats. ● Identify trends and patterns in security incidents based on established guidelines. ● Perform event correlation using collected information to achieve situational awareness and assess threat levels. ● Collect preliminary information about the application through documentation review. ● Utilize automated tools and techniques to gather web-based information. ● Compile application security controls from various internal and external sources. ● Research industry trends related to the application to inform security practices. ● Gather information on application patching and its dependencies with IT infrastructure. ● Classify vulnerabilities and assess their severity, including the sensitivity of the information at risk. ● Capture and log key events and activities using appropriate formats and tools. ● Maintain a tracker for cybersecurity incidents related to applications. ● Analyze application traffic to identify anomalies and threats. ● Identify trends and patterns in security incidents following standard protocols.	interpreting data as specified by the performance criteria. Effective communication is crucial, as the job holder frequently interacts with stakeholders, team members, business users, and security specialists. They must present findings, prepare reports, and manage databases, aligning with several performance criteria outlined in the corresponding qualification. Additionally, the role demands proficiency in problem-solving and critical thinking to address security vulnerabilities and enhance application defenses, ensuring that the security measures are both effective and compliant with industry standards.	

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
Responsibility	● Ensure that all web servers, web applications, and databases are regularly updated and patched according to the latest security guidelines. ● Verify adherence to Security Technical Implementation Guides (STIGs) to ensure compliance with established best practices. ● Collaborate with senior staff to create or follow established security configuration guidelines for hardening applications across various categories. ● Implement mechanisms to ensure timely application of security updates, antivirus software, and patches across all application assets. ● Prioritize service requests based on organizational policies and guidelines. ● Follow up with relevant personnel to ensure prompt action on incidents within agreed-upon timelines. ● Seek assistance from specialists when encountering issues beyond personal expertise or experience. ● Stay informed about the latest industry developments, standards, and advancements in information security tools and techniques.	The job role holder is responsible for assessing and enhancing application security by conducting thorough security testing and monitoring application security measures according to established guidelines. He/she is accountable for identifying and mitigating threats and vulnerabilities in applications, ensuring compliance with security policies. Additionally, the role involves staying updated on emerging security trends and technologies to inform best practices. The analyst is responsible for their own work and learning, actively engaging in continuous professional development to improve their skills. They also play a supportive role in guiding team members, contributing to the overall learning environment within the group, while holding limited responsibility for the outcomes of others' work.	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)	

2	Relevant Software	● Static Application Security Testing (SAST) Tools: SonarQube ● Dynamic Application Security Testing (DAST) Tools: OWASP ZAP ● Software Composition Analysis (SCA) Tools: OWASP Dependency-Check ● Vulnerability Management Platforms: OpenVAS ● Security Orchestration, Automation, and Response (SOAR) Platforms: Cortex XSOAR ● Programming languages like PHP, Java, Python, or Go etc. ● Operating Systems: 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	033-67992222	info@capitalnumbers.com	-

				#2 F/4, AA II, F, Newtown, Kolkata, Chakpachuria, West Bengal 700156			
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,	9325031747	share@konnectgrow.com	-

				Maharashtra 411014			
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	**400-700**	**200-500**	**100-250**		

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 assessment case study-based questions also include 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/N0958: Access API and application for security	PC 1. review and collect initial information about the application from available data	2	2	-	1
	PC 2. assess the importance of information by considering multiple influencing factors like nature of the data, source of the data, size of the data and others	1	2	-	1
	PC 3. identify the application type/category by considering various factors like Programming languages, React, Angular, Spring frameworks and others	1	2	-	1
	PC 4. demonstrate the ability to assess and implement API authentication, authorization, rate limiting, and data validation to ensure secure and efficient API operations	2	2	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 5. conduct targeted assessments to validate and ensure the security of API operations, addressing vulnerabilities related to authentication, authorization, and data integrity	2	2	-	1
	PC 6. implement API gateway security measures, including rate limiting and authentication, to ensure secure and efficient API operations	1	2	-	1
	PC 7. assess applications to identify and address misconfigurations and supply chain vulnerabilities, ensuring alignment with security standards and best practices	1	2	-	1
	PC 8. collect data on application patching and its interdependencies with IT infrastructure needs	1	2	-	1
	PC 9. prioritize vulnerabilities based on business objectives, potential impact, and exploitability	1	4	-	1
	PC 10. secure infrastructure as code (IaC) templates (e.g., Terraform, CloudFormation) by identifying vulnerabilities, applying security best practices, and ensuring compliance with organizational security policies	1	3	-	1
	PC 11. utilize advanced vulnerability scanning tools such as Checkmarx, Veracode, or Snyk to identify security vulnerabilities in applications, analyze the results and mitigate risk	1	3	-	1
	PC 12. evaluate the security of containerized environments (e.g., Docker, Kubernetes) and implement measures to secure serverless functions (e.g., AWS Lambda, Azure Functions) to protect against vulnerabilities and threats	1	2	-	1
	PC 13. utilize PowerShell scripting to enhance application security	1	1	-	1
	PC 14. isolate root causes of vulnerabilities and identify fixes, by including contextual information like architectural composition, exploitation methods, and probabilities of exposure	1	2	-	-
	PC 15. verify data to detect false positives and isolate individual vulnerabilities	2	2	-	1

NOS/Module Name	**Assessment Criteria for Performance Criteria/Learning Outcomes**	**Theory Marks**	**Practical Marks**	**Project Marks**	**Viva Marks**
	PC 16. perform threat modeling to uncover potential vulnerabilities and implement security measures from the outset of software design and architecture	1	2	-	1
	PC 17. create an application tracking system to capture and record essential information	1	1	-	-
	PC 18. develop a plan for application penetration testing that addresses multiple parameters	1	2	-	1
	PC 19. test applications using various testing methods	1	2	-	-
	PC 20. utilize malware sandboxing techniques to analyze and isolate potential threats	2	1	-	1
	PC 21. execute penetration testing by employing automated scanning technologies, black box testing, and manual tests that leverage human insight to inform the process	1	2	-	-
	PC 22. document the security requirements for applications specified by clients and external stakeholders in the designated format throughout the application life cycle	1	2	-	1
	PC 23. record information and activities at each stage to create a comprehensive audit trail	1	1	-	-
	PC 24. ensure the secure storage of data gathered during the assessment, including details on vulnerabilities, analysis findings, and mitigation recommendations	1	2	-	1
	PC 25. automate the integration of results from static, dynamic, and interactive application security testing	1	2	-	1
	Total Marks	**30**	**50**	**0**	**20**
SSC/N0959: Manage application security,	PC 1. locate all web servers and web applications on the network and secure their administrative interfaces	1	2	-	1
	PC 2. confirm that all web servers, web applications, and databases are updated with the latest patches and adhere to Security Technical Implementation Guides (STIGs) to ensure compliance with best practices	1	2	-	-

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
hardening and vulnerability	PC 3. evaluate the list of systems and applications to identify and remove unauthorized instances and unnecessary functionalities to minimize the risk of exploitation	1	2	-	1
	PC 4. illustrate how Active Directory operates	1	2	-	1
	PC 5. detect and address attacks such as Kerberos ticket forging (Kerberos roasting)	1	2	-	-
	PC 6. apply hardening measures to strengthen domain controllers	1	2	-	1
	PC 7. review logs for web attacks and identify signs of compromise	1	2	-	1
	PC 8. implement application and database defenses such as firewalls	1	2	-	1
	PC 9. assess cloud platforms (AWS, Azure, GCP) along with their security features to protect internal servers of the organization	1	2	-	1
	PC 10. evaluate cloud infrastructure for potential vulnerabilities and verify that cloud environments comply with security best practices	1	2	-	1
	PC 11. utilize threat intelligence to identify and respond to emerging threats	1	2	-	1
	PC 12. customize assessments according to current threat data	1	2	-	1
	PC 13. stay informed about the latest threat indicators	1	3	-	1
	PC 14. assess IoT devices and their applications for potential security vulnerabilities like lack of encryption, insecure software updates, lack of authentication and others	1	3	-	1
	PC 15. establish safeguards to protect communications between devices	1	2	-	1
	PC 16. evaluate the security of AI/ML models for vulnerabilities, biases, and potential adversarial attacks	1	3	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 17. ensure that cloud environments comply with security best practices and regularly evaluate and enhance the security posture using Cloud Security Posture Management (CSPM) tools	2	3	-	1
	PC 18. conduct fuzz testing to identify vulnerabilities in APIs and maintain ongoing monitoring for security breaches	1	2	-	-
	PC 19. work alongside development and operations teams to integrate security practices throughout the Software Development Life Cycle (SDLC) and automate security testing within Continuous Integration/Continuous Deployment (CI/CD) pipelines	1	2	-	1
	PC 20. review both frontend and backend platforms for identified vulnerabilities and assess available patches or updates	1	1	-	-
	PC 21. establish a security baseline for malware protection across servers, endpoints, and applications, ensuring regular signature updates and timely application of patch and security updates	2	1	-	-
	PC 22. collaborate with the application development team to identify, analyze, and mitigate security vulnerabilities, ensuring secure deployment and resolution of issues across the organization	1	1	-	1
	PC 23. educate business users on application vulnerabilities and the need for timely patching	3	1	-	1
	PC 24. ensure that IT infrastructure processes are redesigned to align with patch management requirements	1	1	-	-
	PC 25. investigate industry best practices for hardening applications to enhance security	1	1	-	1
	PC 26. record and document the outcomes generated by the tools and solutions implemented	1	2	-	1
	Total Marks	**30**	**50**	**0**	**20**

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
SSC/N0960: Oversee the Cloud security of deployed applications and solutions to detect potential breaches and compromises	PC 1. confirm the scope of application assets and system components to be monitored with relevant authorized personnel	1	2	-	1
	PC 2. execute PowerShell syntax and basic commands effectively to automate tasks and enhance system administration	2	2	-	-
	PC 3. automate routine tasks and perform system administration efficiently by developing and executing security scripts using PowerShell	2	2	-	1
	PC 4. define and establish operational processes for log management	2	2	-	1
	PC 5. identify and capture all the key events and activity logs as per established format using appropriate tools and infrastructure	2	2	-	1
	PC 6. Conduct comprehensive security assessments of applications to identify vulnerabilities, assess potential risks, and ensure protection against threats such as hacking attempts, phishing, malware, and ransomware.	1	2	-	1
	PC 7. Implement and oversee security controls within software development to mitigate risks, ensuring that all applications adhere to industry security standards and protect against potential cyberattacks.	1	2	-	1
	PC 8. Perform real-time monitoring and threat analysis to detect and respond to security breaches, employing techniques to safeguard the organization from malware, ransomware, and other forms of cyber threats.	1	2	-	1
	PC 9. create secure sandbox environments to isolate threats	1	2	-	1
	PC 10. use sandbox environments to analyze malware behavior, detect malicious files, and assess associated risks	2	2	-	1
	PC 11. perform comprehensive analysis to uncover underlying security issues and implement long-term fixes and mitigation strategies to address identified vulnerabilities	2	2	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 12. collaborate with the organization's computer network defense (CND) team to confirm network alerts	1	2	-	1
	PC 13. analyze the information collected to achieve situational awareness and assess the level of threat potential through event correlation	1	2	-	1
	PC 14. classify the urgency of recognized risks by assessing their likelihood of happening and potential consequences according to organizational procedures and policies	1	2	-	-
	PC 15. identify the necessary steps to assess and address recognized risks	1	2	-	1
	PC 16. log incidents in ticketing systems if any suspicious findings arise during the analysis	1	2	-	-
	PC 17. classify the service request according to the organization's processes and policies	1	2	-	-
	PC 18. allocate the ticket to the appropriate individuals based on the type of risk, in accordance with organizational procedures	1	2	-	1
	PC 19. arrange the service requests based on the organization's guidelines	1	2	-	1
	PC 20. coordinate with the appropriate personnel to ensure actions are taken on the tickets raised within the specified timelines	-	2	-	1
	PC 21. seek assistance or guidance from a specialist if the issue falls outside their knowledge or expertise	-	2	-	-
	PC 22. document the outcomes of monitoring, ticket creation, and ticket resolution activities using standardized forms in accordance with organizational protocols	1	2	-	1
	PC 23. adhere to applicable laws, regulations, policies, and guidelines	1	2	-	1
	PC 24. keep track of external data sources, such as CND vendor websites, Computer Emergency Response Teams, SANS, and Security Focus, to identify security issues that could affect the organization	2	2	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC 25. conduct telemetry monitoring to detect issues with the security platform	1	2	-	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 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.