QUALIFICATION FILE

Cloud Security Analyst

☒ Short Term Training (STT) ☐ Long Term Training (LTT) ☒ Apprenticeship

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

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

NCrF/NSQF Level: 6.5

Submitted By:

IT-ITeS Sector Skills Council NASSCOM (SSC NASSCOM)

Plot No. – 7, 8, 9 & 10

Sector – 126, Noida, Uttar Pradesh - 201303

Table of Contents

Section 1: Basic Details

<table>
<tr><td>1.</td><td>Qualification Name</td><td colspan="2">Cloud Security Analyst</td></tr>
<tr><td>2.</td><td>Sector/s</td><td colspan="2">IT/ITeS</td></tr>
<tr><td>3.</td><td>Type of Qualification: ☐ New ☒ Revised ☐ Has Electives/Options ☐OEM</td><td>NQR Code & version of existing/previous qualification: 2022/ITES/ITSSC/06155 & v3.0</td><td>Qualification Name of existing/previous version: Cloud Security Analyst</td></tr>
<tr><td>4.</td><td>a. OEM Name
b. Qualification Name
(Wherever applicable)</td><td colspan="2"></td></tr>
<tr><td>5.</td><td>National Qualification Register (NQR) Code &Version
(Will be issued after NSQC approval)</td><td>QG-6.5-IT-045922025-V2-NASSCOM, v4.0</td><td>6. NCrF/NSQF Level: 6.5</td></tr>
<tr><td>7.</td><td>Award (Certificate/Diploma/Advance Diploma/ Any Other (Wherever applicable specify multiple entry/exits also & provide details in annexure)</td><td colspan="2">Certificate</td></tr>
<tr><td>8.</td><td>Brief Description of the Qualification</td><td colspan="2">A Cloud Security Analyst ensures that cloud operations align with organizational policies, regulatory requirements, and industry standards. The individual assesses cloud security risks, defines and monitors security controls, conducts audits, coordinates incident response, and tracks compliance through defined KPIs. The person supports secure and compliant cloud adoption across the organization.</td></tr>
<tr><td>9.</td><td>Eligibility Criteria for Entry for Student/Trainee/Learner/Employee</td><td colspan="2">a. Entry Qualification & Relevant Experience:
<table>
<tr><th>S. No.</th><th>Academic/Skill Qualification (with Specialization - if applicable)</th><th>Required Experience (with Specialization - if applicable)</th></tr>
<tr><td>1.</td><td>Completed 1-year PG*</td><td></td></tr>
<tr><td>2.</td><td>Completed 4-year UG*</td><td>1.5 -year relevant experience</td></tr>
<tr><td>3.</td><td>Previous relevant Qualification of NSQF Level 6.0</td><td>1.5-year relevant experience</td></tr>
<tr><td>4.</td><td>Previous relevant Qualification of NSQF Level 5.5</td><td>3-year relevant experience</td></tr>
</table>
*UG/PG in Computer Science/ Information Technology/ Electrical and Electronics Engineering.
**Relevant Experience in cloud application development or DevOps</td></tr>
<tr><td>10.</td><td>Credits Assigned to this Qualification, Subject to Assessment (as per National Credit Framework (NCrF))</td><td>23</td><td>11. Common Cost Norm Category (I/II/III) (wherever applicable): II</td></tr>
</table>

<table>
<tr><td>12.</td><td>Any Licensing requirements for Undertaking Training on This Qualification (wherever applicable)</td><td colspan="2">NA</td></tr>
<tr><td>13.</td><td>Training Duration by Modes of Training Delivery (Specify Total Duration as per selected training delivery modes and as per requirement of the qualification)</td><td colspan="2">☐Offline ☐Online ☒Blended
<table><tr><th>Training Delivery Modes</th><th>Theory (Hours)</th><th>Practical (Hours)</th><th>OJT Mandatory (Hours)</th><th>OJT Recommended (Hours)</th><th>Total (Hours)</th></tr><tr><td>Classroom (offline)</td><td>204</td><td>336</td><td>150</td><td></td><td rowspan="2">690</td></tr><tr><td>Online</td><td>204</td><td>336</td><td>150</td><td></td></tr></table>(Refer Blended Learning Annexure for details)</td></tr>
<tr><td>14.</td><td>Aligned to NCO/ISCO Code/s (if no code is available mention the same)</td><td colspan="2">NCO-2015/2522.0201</td></tr>
<tr><td>15.</td><td>Progression path after attaining the qualification (Please show Professional and Academic progression)</td><td colspan="2">Senior Cloud Security Analyst</td></tr>
<tr><td>16.</td><td>Other Indian languages in which the Qualification & Model Curriculum are being submitted</td><td colspan="2">Hindi</td></tr>
<tr><td>17.</td><td>Is similar Qualification(s) available on NQR-if yes, justification for this qualification</td><td colspan="2">☐ Yes ☒ No URLs of similar Qualifications:</td></tr>
<tr><td>18.</td><td>Is the Job Role Amenable to Persons with Disability</td><td colspan="2">☒ Yes ☐ No
If “Yes”, specify applicable type of Disability: Locomotor Disability</td></tr>
<tr><td>19.</td><td>How Participation of Women will be Encouraged</td><td colspan="2">To encourage women to pursue careers in cloud computing, it is essential to provide targeted education, mentorship, and upskilling opportunities focused on cloud technologies. Training programs, industry certifications, and access to professional networks can help build both confidence and expertise. Flexible work arrangements and the visibility of successful women in cloud computing can serve as powerful motivation. Furthermore, fostering a culture of inclusion and diversity—through equitable policies on work-life balance, equal pay, promotion opportunities, and a safe, respectful workplace—can help women feel supported, valued, and empowered in the cloud computing industry.</td></tr>
<tr><td>20.</td><td>Are Greening/ Environment Sustainability Aspects Covered (Specify the NOS/Module which covers it)</td><td colspan="2">☒ Yes ☐ No
(Covered in DGT/VSQ/N0102)</td></tr>
<tr><td>21.</td><td>Is Qualification Suitable to be Offered in Schools/Colleges</td><td colspan="2">Schools ☐ Yes ☒ No Colleges ☒ Yes ☐ No</td></tr>
<tr><td>22.</td><td>Name and Contact Details of Submitting / Awarding Body SPOC
(In case of CS or MS, provide details of both Lead AB & Supporting ABs)</td><td colspan="2">Name: Namrata Kapur
Email: standards@nasscom.in Contact No.: 0120-4990111
Website: https://www.sscnasscom.com/</td></tr>
<tr><td>23.</td><td>Final Approval Date by NSQC: 07/10/2025</td><td>24. Validity Duration: 3 Years</td><td>25. Next Review Date: 07/10/2028</td></tr>
</table>

Section 2: Module Summary

NOS/s of Qualifications

(In exceptional cases these could be described as components)

Mandatory NOS/s:

Specify the training duration and assessment criteria at NOS/ Module level. For further details refer curriculum document.

***Th.**-Theory **Pr.**-Practical **OJT**-On the Job Training **Man.**-Mandatory **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.	Develop an organizational understanding to manage cloud security risks	SSC/N8332, v3.0	Core	6.5	5	60	60	30	-	150	30	50	-	20	100	20
2.	Define, monitor and manage cloud security safeguards and policies in the organization	SSC/N8333, v3.0	Core	6.5	4	30	60	30	-	120	30	50	-	20	100	20
3.	Audit IT and cloud assets and identify KPIs to monitor implementation of governance standards	SSC/N8326, v3.0	Core	6.5	4	30	60	30	-	120	30	50	-	20	100	20
4.	Coordinate response to cloud security incidents and ensure restoration of affected systems	SSC/N8335, v3.0	Core	6.5	4	30	60	30	-	120	30	50	-	20	100	15
5.	Ensure compliance with legal, regulatory, and certification standards applicable to cloud systems	SSC/N8336, v3.0	Core	6.5	4	30	60	30	-	120	30	50	-	20	100	15
6.	Employability Skills (60 Hours)	DGT/VSQ/N0102, v1.0	Non-Core	4.0	2	24	36	-	-	60	20	30	-	-	50	10
Duration (in Hours) / Total Marks					**23**	**204**	**336**	**150**		**690**	**170**	**280**	**-**	**100**	**550**	**100**

Assessment - Minimum Qualifying Percentage

*Please specify **any one** of the following:*

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.)*

Minimum Pass Percentage – NOS/Module-wise: - % *(Every Trainee should score specified minimum passing percentage in each mandatory and selected elective NOS/Module 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 Engineering/Technology/ Statistics/ Mathematics/Computer Science. **Industry & Training Experience:** 2 years of industry experience IT/Computer science/Cloud Computing domain. **Certification:** "Trainer" mapped to the Qualification Pack "MEP/Q2601, v3.0" 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 Engineering/Technology/ Statistics/ Mathematics/Computer Science. **Industry & Training Experience:** 4 years of industry experience IT/Computer science/Cloud Computing domain. **Certification:**" Master Trainer" mapped to the Qualification Pack "MEP/Q2602, v3.0" Minimum accepted score is 90% aggregate.
3.	**Tools and Equipment Required for 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 Engineering/Technology/ Statistics/ Mathematics/Computer Science. **Industry & Training Experience:** 2 years of industry experience IT/Computer science/Cloud Computing domain. **Certification:** "Assessor" mapped to the Qualification Pack "MEP/Q2701, v3.0" Minimum accepted score is 80% aggregate.
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	**Educational Qualification:** Graduate in Engineering/Technology/ Statistics/ Mathematics/Computer Science.

		Industry & Training Experience: 2 years of industry experience IT/Computer science/Cloud Computing domain. **Certification:** "Assessor" mapped to the Qualification Pack "MEP/Q2701, v3.0" 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 Engineering/Technology/ Statistics/ Mathematics/Computer Science. **Industry & Training Experience:** 4 years of industry experience IT/Computer science/Cloud Computing domain. **Certification:** "Lead Assessor" mapped to the Qualification Pack "MEP/Q2702, v3.0" Minimum accepted score is 90% aggregate.
4.	**Assessment Mode** *(Specify the assessment mode)*	The assessment will consist of a blend of hands-on practical evaluations, viva-voce, and online proctored scenario-based multiple-choice questions ensuring a thorough evaluation of the individual's proficiency in learning outcomes, practical understanding, and real-world application of concepts.
5.	**Tools and Equipment Required for Assessment**	☒ Same as for training ☐ Yes ☐ No *(details to be provided in Annexure-if it is different for Assessment)*

Section 5: Evidence of the need for the Qualification

Provide Annexure/Supporting documents name.

1.	**Latest Skill Gap Study (not older than 2 years) (Yes/No):** Yes
2.	**Latest Market Research Reports or any other source (not older than 2 years) (Yes/No):** NA
3.	**Government /Industry initiatives/ requirement (Yes/No):** NA
4.	**Number of Industry validation provided:** 21
5.	**Estimated nos. of persons to be trained and employed:** 1000
6.	**Evidence of Concurrence/Consultation with Line Ministry/State Departments:** *In Process* 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 level/NSQF descriptors *(Mandatory)*	*Annexure 1*
2.	**Annexure:** List of tools and equipment relevant for qualification *(Mandatory, except in case of online course)*	*Annexure 2*

3.	**Annexure:** Detailed Assessment Criteria *(Mandatory)*	*Annexure 6*
4.	**Annexure:** Assessment Strategy *(Mandatory)*	*Annexure 7*
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)*	*NA*
7.	**Annexure:** Acronym and Glossary *(Optional)*	*Annexure 8*
8.	**Supporting Document:** Model Curriculum *(Mandatory – Public view)*	*Attached*
9.	**Supporting Document:** Career Progression *(Mandatory - Public view)*	*Attached*
10.	**Supporting Document:** Occupational Map *(Mandatory)*	*Attached*
11.	**Supporting Document:** Assessment SOP *(Mandatory)*	*Attached*
12.	**Any other document you wish to submit:**	*N0*

Annexure 1: 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	**Assess and Manage Cloud Security Risks** • Identify IT and cloud assets by criticality and business impact. • Conduct threat and vulnerability assessments using automated tools. • Analyze risks using frameworks like NIST, ISO/IEC 27001. **Define and Implement Security Safeguards** • Establish cloud-specific security policies and controls. • Implement access control, encryption, and threat mitigation mechanisms. • Configure and monitor automated tools for threat detection. **Monitor and Audit Cloud Environments** • Conduct periodic audits using industry checklists and tools. • Define and track KPIs to monitor governance and compliance. • Use AI/ML to detect anomalies, misconfigurations, or policy drift.	The job role of a Cloud Security Analyst involves in-depth theoretical knowledge of cloud infrastructure, security frameworks, threat modeling, compliance standards, and incident response strategies. It requires an analytical understanding of advanced concepts such as shared responsibility models, AI/ML-enabled security analytics, and real-time anomaly detection across cloud environments. The role demands structured application of complex processes including risk assessment, audit preparation, policy enforcement, and continuous compliance monitoring. This aligns well with Level 6.5, where the application of advanced theoretical and procedural knowledge is essential to managing critical cloud security functions.	6.5

	Respond to Security Incidents • Develop and execute automated incident response strategies. • Classify, escalate, and document security events. • Ensure timely recovery and post-incident analysis for improvement. **Ensure Legal, Regulatory, and Certification Compliance** • Interpret and implement global compliance standards (e.g., GDPR, HIPAA, PCI-DSS). • Coordinate internal and third-party audits for certification. • Monitor policy enforcement and regulatory adherence using digital tools. **Leverage AI/ML for Security Operations** • Use AI-enabled SIEM and SOAR tools for monitoring and automated response. • Train ML models to predict threat patterns and optimize response strategies. • Analyze logs and behaviors for advanced threat detection.		
Professional and Technical Skills/ Expertise/ Professional Knowledge	• Strong understanding of cloud security frameworks and shared responsibility models. • Knowledge of vulnerability testing, threat modeling, and incident classification. • Familiarity with compliance standards like ISO/IEC 27001, NIST, GDPR, HIPAA, PCI-DSS. • Proficiency in security monitoring tools (e.g., AWS GuardDuty, Azure Sentinel, Splunk). • Competence in AI/ML integration for anomaly detection, risk prediction, and automated incident handling. • Ability to define and monitor cloud-specific KPIs for governance and risk. • Skill in developing and managing security runbooks, checklists, and incident response playbooks. • Knowledge of audit protocols, compliance documentation, and regulatory reporting formats. • Understanding of cloud platforms (AWS, Azure, GCP) and their native security services. • Expertise in policy creation, enforcement automation, and secure configurations.	This job role requires highly specialized skills in auditing, cloud-specific risk mitigation, compliance enforcement, and automated security operations. It includes the ability to define and apply regulatory standards (e.g., ISO/IEC 27001, GDPR), implement technical controls (IAM, encryption, logging), use AI/ML models for pattern detection, and interpret complex security telemetry. The Cloud Security Analyst is expected to independently evaluate, prioritize, and respond to evolving threats while working across internal teams and external vendors. These technical and decision-making abilities, along with operational leadership in security, strongly align with Level 6.5 expectations of expertise and autonomy in complex environments.	6.5

	• Technical skills in SIEM, SOAR, IAM, endpoint protection, and encryption protocols. • Ability to support certification processes (e.g., SOC 2, ISO/IEC certifications).		
Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	• Demonstrate ethical judgment and adherence to privacy and legal standards. • Apply critical thinking and problem-solving during security breaches and audits. • Exhibit accountability and ownership over compliance and security posture. • Communicate clearly with cross-functional teams and regulatory authorities. • Show adaptability to new tools, evolving threats, and policy changes. • Maintain attention to detail when documenting findings or reporting incidents. • Collaborate across departments and vendors to ensure unified security strategy. • Promote proactive learning and stay current on emerging cybersecurity trends	A Cloud Security Analyst must demonstrate forward-thinking judgment, ethical decision-making, and strong communication skills in high-stakes situations involving data breaches or compliance gaps. The role demands initiative, a sense of ownership in enforcing security posture, adaptability to rapidly evolving technologies, and accountability in managing cross-functional security incidents. The analyst must collaborate with diverse teams while upholding confidentiality, legal compliance, and strategic alignment with business goals — reflecting the leadership, self-direction, and professional mindset characteristic of Level 6.5.	6.5
Broad Learning Outcomes/Core Skill	• Evaluate and prioritize cloud assets for risk-based security planning. • Design and implement security controls aligned with cloud environments. • Monitor, analyze, and audit cloud configurations and compliance status. • Respond efficiently to incidents with predefined, automated workflows. • Apply AI/ML for advanced analytics in security and compliance operations. • Facilitate internal and external audits with complete documentation and evidence. • Communicate effectively to ensure alignment among teams, vendors, and regulators. • Demonstrate technical and legal understanding to manage certification and policy enforcement.	The role requires synthesizing technical risk data, evaluating incident trends, and aligning security responses with business impact. It includes the capability to design scalable policies, audit systems proactively, and support secure digital transformation through governance and continuous monitoring. The analyst must apply analytical reasoning and critical thinking to secure diverse cloud environments, demonstrating the integration of deep theoretical understanding with applied problem-solving skills. These learning outcomes exemplify the complex reasoning and adaptable core competencies outlined at Level 6.5.	6.5

Responsibility	The individual in this job role will be responsible for the below-mentioned activities: • Identifying and classifying risks to cloud assets and operations. • Establishing and maintaining cloud security policies and procedures. • Monitoring cloud environments using tools and AI for threats and compliance gaps. • Coordinating incident response and documenting investigation outcomes. • Supporting compliance with legal, regulatory, and certification standards. • Planning and participating in internal and external audits. • Updating security configurations and policies based on audit findings and threat evolution. • Educating teams on cloud security best practices and protocols. • Using digital tools for governance tracking, reporting, and automated enforcement. • Collaborating with vendors and internal departments to uphold secure, compliant operations.	A Cloud Security Analyst ensures that cloud operations align with organizational policies, regulatory requirements, and industry standards. The individual assesses cloud security risks, defines and monitors security controls, conducts audits, coordinates incident response, and tracks compliance through defined KPIs. The person supports secure and compliant cloud adoption across the organization.	6.5

Annexure 2: Tools and Equipment (Lab Set-Up)

List of Tools and Equipment

Batch Size: 30

S. No.	Tool / Equipment Name	Specification	Quantity for specified Batch size
1.	Cloud pricing tools (e.g., AWS Pricing Calculator, Azure Pricing Tool, Google Cloud Pricing Calculator)		
2.	Cloud monitoring and observability tools (e.g., Amazon CloudWatch, Prometheus, Datadog, Azure Monitor)		
3.	Security tools (e.g., IAM tools, MFA tools, vulnerability scanners, firewall configurations)		
4.	Container orchestration tools (e.g., Kubernetes, Docker Swarm)		

5.	Cloud vendor platforms (e.g., AWS, Microsoft Azure, Google Cloud Platform)		
6.	Version control and documentation tools (e.g., Git, Confluence)		

*Tools are open source

Classroom Aids

The aids required to conduct sessions in the classroom are:

1. Whiteboard
2. Projector
3. Computer/Laptop
4. Chairs
5. Tables
6. Whiteboard marker
7. Duster

Annexure 3: Industry Validations Summary

Provide the summary information of all the industry validations 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.	Reckitt Benckiser	Sachin Sharma	Demand Manager	Udyog Vihar, Phase V, Gurgaon, Haryana	9758573077	Sachin.Sharma@rb.com	
2.	PwC India	Yatharth Bhatnagar	Software Engineer	Pune	7276325777	yatharth23@gmail.com	
3.	Dell Technologies	Ariba Syed	Software Engineer	Surat		ariba.syed2017@gmail.com	
4.	Movate	Rohit Kumar Sharma	Manager – Development	A-21, sector 4, Block A, Kailash Colony, Greater Kailash, New Delhi,	9927564461	rohit.sharma.movate@gopangea.com	
5.	Nasdaq Inc	Alfiya Khan	Software Engineer	Unit 201 and 203, Akruti Center Point, MIDC Road, Andheri (East) Mumbai: 400-093, India.	8109690056	alfiya.Khan@Nasdaq.com	

6.	Getronics Solutions India Private Limited	Devendra Prasad	Team Lead - Quality & Performance	Gurgaon	9711592810	devprasad83@gmail.com	
7.	Nagarro	Firoz Zaidi	Senior Developer	Noida	8218191014	firoz@nagarro.com	
8.	Tata Consultancy Services	Ankit Garg	Assistant Consultant	Gurgaon	9808254808	ankit.garg8@tcs.com	
9.	T-Systems ICT India Pvt Ltd	Monica Sharma	Sr. Consultant	Pune	7389777739	monica.sharma@t-systems.com	
10.	Michelin India Private Ltd.	Himanshu Sharma	Business Analyst/Product Owner	Pune		sharmaaz.himanshu@gmail.com	
11.	Siemens Digital Industries Software	Snehal Pandey	Software Engineer	Pune	7387151993	snehalpande93@gmail.com	
12.	Deloitte Support Services Private Limited	Shreya Sharma	Senior Analyst (PMO)	Hyderabad Deloitte Towers, Mindspace Road, P Janardhan Reddy Nagar, Gachibowli, Hyderabad, Telangana 500032	8999530108	shreyasharma5@deloitte.com	
13.	PwC India	Ruchita Panchal	Senior Consultant	Gurgaon	7354047944	ruchita.panchal@pwc@gmail.com	
14.	Conduent	Prince Jain	Sr. Business Analyst	Noida	9013 241797	prince.jain@conduent.com	
15.	Tata Consultancy Services	Sheepra Kaushik	Associate Consultant	Mumbai, India	8433595090	sheepra.sharma@tcs.com	
16.	Infosys Ltd.	Yash Kumawat	Senior product engineer	Bengaluru	8319749784	yash120997@gmail.com	
17.	Capgemini	Shruti Gupta	Manager	Chennai, Tamil Nadu, India	9004343572	shrutivijendra@gmail.com	
18.	Protiviti Global Business Consulting	Sakshi Samtani	Senior Manager	Mumbai	8080536463	sakshi3192@gmail.com	
19.	HCL Tech	Sheeloo Sachan	Technical Specialist	Plot No 3A, Sector 126, Noida, Uttar Pradesh 201301	9717036547	sachan.sheeloo@gmail.com	
20.	Infosys Ltd	Shraddha Sethiya	Technology Analyst	No. 44 & 97/A, Infosys Avenue, Next SBI Bank, Hosur Road, Electronic City-Bengaluru 560100, Karnataka, India	99267854201	shraddha.sethiya@infosys.com	
21.	Sycamore Informatics	Rahul Kumar Kaushik	Product Manager	No. 6, 2nd Floor, 2nd Main, Arekere, Off Bannerghatta	8859885973	rahul.kaushik@sycamoreinformatics.com	

				Road, Bangalore 560076			

Annexure 4: Training & Employment Details

Training and Employment Projections:

Year	Total Candidates		Women		People with Disability	
	Estimated Training #	Estimated Employment Opportunities	Estimated Training #	Estimated Employment Opportunities	Estimated Training #	Estimated Employment Opportunities
2024	200	75	10	5	5	5
2025	300	100	15	10	10	10
2026	500	200	25	10	10	10

Data to be provided year-wise for 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	Placed	Trained	Assessed	Certified	Placed	Trained	Assessed	Certified	Placed
V3.0	2024												
V3.0	2023												
V3.0	2022												

Applicable for revised qualifications only, data to be provided year-wise for past 3 years.

List Schemes in which the previous version of Qualification was implemented:

1.
2.

Content availability for previous versions of qualifications:

☒ Participant Handbook ☒ Facilitator Guide ☒ Digital Content ☐ Qualification Handbook ☐ Any Other:

Languages in which Content is available: English and Hindi

Annexure 5: 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	▪ Books/ e-books ▪ Presentations ▪ Reference Material ▪ Audio / Video Modules	
2	☒Imparting Soft Skills, Life Skills, and Employability Skills /Mentorship to Learners	▪ Self-Learning Videos (optional) ▪ Broadcasts (optional) ▪ Mobile Learning ▪ Curated Digital content (optional)	
3	☒Showing Practical Demonstrations to the learners	▪ Video Content (optional) ▪ E-Resource library (optional)	
4	☒Imparting Practical Hands-on Skills/ Lab Work/ workshop/ shop floor training	▪ Training tools (tools list attached) ▪ Video Play ▪ Presentations	
5	☒Tutorials/ Assignments/ Drill/ Practice	▪ Online Question Bank ▪ MCQ based tests	
6	☒Proctored Monitoring/ Assessment/ Evaluation/ Examinations	▪ Assessment engine for Essays (optional) ▪ Mock test sessions	
7	☒On the Job Training (OJT)/ Project Work Internship/ Apprenticeship Training	▪ Online tests ▪ Offline assessments	

Annexure 6: Detailed Assessment Criteria

Detailed assessment criteria for each NOS/Module are as follows:

Proctor online assessment and case study base questions are included.

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
SSC/N8332: Develop an organizational	*Prioritize IT assets and ensure their security*	*8*	*14*	*-*	*5*
	PC1. identify and prioritize IT assets of the organization based on their security and business criticality	2	4	-	1

understanding to manage cloud security risks	PC2. determine shared security responsibilities between internal teams and external service providers	2	3	-	1
	PC3. identify system users and their respective access privileges to IT assets	2	3	-	1
	PC4. collect and analyze historical data on past security incidents from organizational records	2	4	-	2
	Assess threats and vulnerabilities	*10*	*14*	*-*	*6*
	PC5. implement automated security assessment tools to identify threats and vulnerabilities in cloud systems	3	4	-	2
	PC6. conduct vulnerability testing and risk analysis to identify and assess potential security breaches	2	3	-	1
	PC7. evaluate the potential impact of identified threats and vulnerabilities on business operations	3	3	-	2
	PC8. record, classify, and prioritize security incidents using standard templates and tools	2	4	-	1
	Analyze risks and identify anomalies	*12*	*22*	*-*	*9*
	PC9. determine the level of risk for each identified threat and vulnerability	2	4	-	2
	PC10. analyze the effectiveness of current technical and procedural controls in place to mitigate identified threats	2	5	-	1
	PC11. monitor regularly for anomalies and suspicious incidents related to cloud or IT security	2	5	-	2
	PC12. use Artificial Intelligence (AI)/Machine Learning (ML) models to detect anomalous patterns and deviations in cloud activity logs	2	3	-	1
	PC13. utilize machine learning techniques to improve the accuracy of threat prediction and risk scoring over time	2	3		1
	PC14. develop Key Performance Indicators (KPIs) to track and report security incidents and trends over time	2	2		2
	Total Marks	**30**	**50**	**-**	**20**
SSC/N8333: Define, monitor and manage cloud security safeguards and policies in the organization	*Conduct preliminary security analysis*	*7*	*12*	*-*	*6*
	PC1. create and maintain reports on actual or potential cloud security threats and incidents	1	4	-	1
	PC2. analyze the shared cloud security model based on service provider type and deployment architecture	2	2	-	1
	PC3. identify and configure automated tools to perform routine security assessments of cloud systems	2	2		2
	PC4. evaluate the likelihood and potential impact of anomalies identified through security monitoring	1	2		1
	PC5. apply security controls in line with established policies to detect unauthorized or unusual activity	1	2		1
	Define cloud-related security policies and safeguards	*10*	*17*	*-*	*7*
	PC6. define organizational responsibilities for securing cloud infrastructure and applications	1	4	-	1
	PC7. formulate and document policies for access control, encryption, and threat mitigation	2	2	-	1

	PC8. select and implement cloud-specific security standards (e.g., ISO/IEC 27017, 27018) relevant to the organization	1	3	-	1
	PC9. establish and maintain governance processes for the enforcement of cloud security measures	2	2	-	1
	PC10. integrate applicable data protection and privacy regulations into cloud security policies	2	2	-	1
	PC11. evaluate and revise existing security guidelines based on threat landscape changes and audit findings	1	2	-	1
	PC12. develop and maintain security checklists, runbooks, and playbooks to guide consistent operational response	1	2	-	1
	Monitor security threats and anomalies	*13*	*21*	*-*	*7*
	PC13. monitor systems using security tools to ensure continuous compliance with defined security policies and standards	2	3	-	1
	PC14. monitor and analyze cloud environment for emerging threats, anomalies, or incidents	2	3	-	1
	PC15. develop and apply Key Performance Indicators (KPIs) to assess the effectiveness of cloud security measure	1	3	-	1
	PC16. use analytics to identify potential attack trends and recommend preventive measures	2	3	-	1
	PC17. integrate AI-powered security tools for continuous monitoring of cloud environments	2	3	-	1
	PC18. apply machine learning-based insights to fine-tune cloud security policies and controls	2	3	-	1
	PC19. report security threats, vulnerabilities, or anomalies to appropriate stakeholders for timely action	2	3	-	1
	Total Marks	**30**	**50**	**-**	**20**
SSC/N8326: Audit IT and cloud assets and identify KPIs to monitor implementation of governance standards	*Audit the organization's IT and cloud assets*	*11*	*19*	*-*	*9*
	PC1. create, maintain, and update a checklist of IT and cloud assets targeted for audit	2	3	-	1
	PC2. liaise with relevant stakeholders to collect data and information required for audits	1	2	-	1
	PC3. conduct audits using approved tools, templates, and checklists in accordance with defined procedures	1	3		2
	PC4. document audit findings, including detected security anomalies or vulnerabilities, and share with appropriate stakeholders	2	3		1
	PC5. maintain updated records of IT and cloud assets, their configurations, and audit status	2	2		1
	PC6. identify the need for a security audit based on prior incidents, threat patterns, or risk indicators	1	2	-	1
	PC7. collect and analyze cloud infrastructure data to verify adherence to compliance and security best practices	1	2	-	1
	PC8. evaluate system configurations and flag deviations from regulatory requirements or organizational standards	1	2	-	1
	Implement and monitor governance standards	*13*	*22*	*-*	*8*

	PC9. apply relevant governance and security standards during the audit process to assess compliance	2	3	-	1
	PC10. define and track Key Performance Indicators (KPIs) to monitor the effectiveness of governance and security control implementation	2	2	-	1
	PC11. use monitoring tools and techniques to assess real-time compliance and detect deviations	2	3	-	1
	PC12. use AI-enabled audit tools to detect patterns of non-compliance or configuration drift	1	2	-	1
	PC13. identify and deploy compatible automated tools for continuous compliance monitoring	1	3	-	1
	PC14. analyze audit logs using ML algorithms to uncover recurring security gaps or compliance issues	1	3	-	1
	PC15. provide timely feedback on detected compliance risks and misconfigurations to support corrective action	2	3	-	1
	PC16. support internal initiatives to strengthen regulatory compliance and enforce policy adherence	2	3	-	1
	Set governance targets and optimize assets	*6*	*9*	*-*	*3*
	PC17. establish governance and operational targets related to performance, cost-efficiency, and security risk mitigation	2	3	-	1
	PC18. optimize utilization of IT and cloud assets based on audit insights to support capacity planning and future budgeting	2	3	-	1
	PC19. recommend or initiate corrective or automated remediation actions for resolving compliance issues	2	3	-	1
	Total Marks	**30**	**50**	**-**	**20**
SSC/N8335: Coordinate response to cloud security incidents and ensure restoration of affected systems	*Coordinate incident response activities and ensure policy alignment*	*12*	*21*	*-*	*7*
	PC1. develop and execute response strategies for detected security incidents in line with compliance requirements and organizational policies	2	4	-	1
	PC2. implement automated or predefined incident response workflows to contain and mitigate active threats	2	3	-	1
	PC3. validate that incident response activities align with approved security standards, procedures, and runbooks	2	4	-	1
	PC4. integrate AI-powered SOAR tools to automate incident triage and response workflows	2	3	-	1
	PC5. use ML models to recommend response actions based on incident classification and past remediation patterns	2	3	-	2
	PC6. review and periodically update incident response documentation, including playbooks and checklists, based on recent incidents and audits	2	4	-	1
	Escalate and report security incidents	*10*	*15*	*-*	*7*
	PC7. assign and escalate information security incidents to designated personnel or teams based on severity and SLA guidelines	2	3	-	1
	PC8. track incident resolution progress, escalate delays or failures, and ensure response timelines are met	2	3	-	2

	PC9. engage relevant internal stakeholders and external vendors to collect and verify incident-related data	2	3	-	1
	PC10. coordinate with management to prepare reports for regulatory bodies or law enforcement, if required	2	3	-	1
	PC11. prepare and submit comprehensive incident reports using approved tools and reporting frameworks	2	3	-	2
	Restore affected cloud systems and update response knowledge base	*8*	*14*		*6*
	PC12. implement containment and isolation measures to prevent escalation of the security incident	2	4	-	2
	PC13. oversee recovery activities and ensure the timely restoration of affected cloud services, configurations, and data	2	4		2
	PC14. verify backup integrity and execute recovery procedures in compliance with organizational guidelines	2	3		1
	PC15. document the response process and lessons learned, and update the organization's knowledge base with post-incident analysis	2	3	-	1
	Total Marks	**30**	**50**	**-**	**20**
SSC/N8336: Ensure compliance with legal, regulatory, and certification standards applicable to cloud systems	*Conduct business analysis*	*3*	*5*	*-*	*3*
	PC1. analyze the organization's business model and industry-specific compliance obligations	1	3	-	2
	PC2. identify applicable regulatory standards, data privacy requirements, and security mandates based on geography, industry, and technology stack	2	2	-	1
	Implement regulatory/compliance requirements	*16*	*24*	*-*	*10*
	PC3. define and document corporate policies to address applicable legal and regulatory standards	2	3	-	1
	PC4. plan and execute compliance-related operational activities across cloud systems	2	3	-	1
	PC5. implement automated compliance monitoring tools compatible with organizational systems	2	3	-	1
	PC6. monitor system configurations to ensure adherence to defined security and compliance benchmarks	2	3	-	1
	PC7. collect and review documentation to validate ongoing compliance with established standards	2	3	-	1
	PC8. analyze misconfigurations or violations to assess associated risk exposure	2	3	-	2
	PC9. recommend or initiate corrective actions, including automated remediation controls for non-compliance	2	3	-	2
	PC10. provide security and compliance-related inputs during vendor selection, contracting, and agreement reviews	2	3	-	1
	Facilitate regulatory/compliance audits	*5*	*9*	*-*	*3*
	PC11. coordinate and support internal and third-party audits to evaluate compliance status	2	3	-	1
	PC12. identify compliance gaps and present issues to relevant stakeholders for prioritization and mitigation	2	3	-	1

	PC13. ensure that compliance processes are audit-ready with appropriate documentation and controls	1	3	-	1
	Ensure regulatory/compliance certification	*6*	*12*	*-*	*4*
	PC14. ensure the organization meets certification requirements set by regulatory authorities	2	2	-	1
	PC15. collaborate with certification bodies to submit compliance reports and obtain necessary approvals	1	4	-	1
	PC16. validate that cloud vendors and third-party partners hold relevant compliance certifications	2	4	-	1
	PC17. create and manage a budget for audit and certification-related activities	1	2	-	1
	Total Marks	**30**	**50**	**-**	**20**
DGT/VSQ/N0102: Employability Skills (60 Hours)	*Introduction to Employability Skills*	*1*	*1*	*-*	*-*
	PC1. identify employability skills required for jobs in various industries	-	-	-	-
	PC2. identify and explore learning and employability portals	-	-	-	-
	Constitutional values – Citizenship	*1*	*1*	*-*	*-*
	PC3. recognize the significance of constitutional values, including civic rights and duties, citizenship, responsibility towards society etc. and personal values and ethics such as honesty, integrity, caring and respecting others, etc.	-	-	-	-
	PC4. follow environmentally sustainable practices	-	-	-	-
	Becoming a Professional in the 21st Century	*2*	*4*	*-*	*-*
	PC5. recognize the significance of 21st Century Skills for employment	-	-	-	-
	PC6. practice the 21st Century Skills such as Self-Awareness, Behaviour Skills, time management, critical and adaptive thinking, problem-solving, creative thinking, social and cultural awareness, emotional awareness, learning to learn for continuous learning etc. in personal and professional life	-	-	-	-
	Basic English Skills	*2*	*3*	*-*	*-*
	PC7. use basic English for everyday conversation in different contexts, in person and over the telephone	-	-	-	-
	PC8. read and understand routine information, notes, instructions, mails, letters etc. written in English	-	-	-	-
	PC9. write short messages, notes, letters, e-mails etc. in English	-	-	-	-
	Career Development & Goal Setting	*1*	*2*	*-*	*-*
	PC10. PC10. understand the difference between job and career	-	-	-	-
	PC11. PC11. prepare a career development plan with short- and long-term goals, based on aptitude	-	-	-	-
	Communication Skills	*2*	*2*	*-*	*-*

	PC12. follow verbal and non-verbal communication etiquette and active listening techniques in various settings	-	-	-	-
	PC13. work collaboratively with others in a team	-	-	-	-
	Diversity & Inclusion	*1*	*2*	-	-
	PC14. communicate and behave appropriately with all genders and PwD	-	-	-	-
	PC15. escalate any issues related to sexual harassment at workplace according to POSH Act	-	-	-	-
	Financial and Legal Literacy	*2*	*3*	-	-
	PC16. select financial institutions, products and services as per requirement	-	-	-	-
	PC17. carry out offline and online financial transactions, safely and securely	-	-	-	-
	PC18. identify common components of salary and compute income, expenses, taxes, investments etc.	-	-	-	-
	PC19. identify relevant rights and laws and use legal aids to fight against legal exploitation	-	-	-	-
	Essential Digital Skills	*3*	*4*	-	-
	PC20. operate digital devices and carry out basic internet operations securely and safely	-	-	-	-
	PC21. use e- mail and social media platforms and virtual collaboration tools to work effectively	-	-	-	-
	PC22. use basic features of word processor, spreadsheets, and presentations	-	-	-	-
	Entrepreneurship	*2*	*3*	-	-
	PC23. identify different types of Entrepreneurship and Enterprises and assess opportunities for potential business through research	-	-	-	-
	PC24. develop a business plan and a work model, considering the 4Ps of Marketing Product, Price, Place and Promotion	-	-	-	-
	PC25. identify sources of funding, anticipate, and mitigate any financial/ legal hurdles for the potential business opportunity	-	-	-	-
	Customer Service	*1*	*2*	-	-
	PC26. identify different types of customers	-	-	-	-
	PC27. identify and respond to customer requests and needs in a professional manner	-	-	-	-
	PC28. follow appropriate hygiene and grooming standards	-	-	-	-
	Getting ready for apprenticeship & Jobs	*2*	*3*	-	-
	PC29. create a professional Curriculum vitae (Résumé)	-	-	-	-
	PC30. search for suitable jobs using reliable offline and online sources such as Employment exchange, recruitment agencies, newspapers etc. and job portals, respectively	-	-	-	-

	PC31. apply to identified job openings using offline /online methods as per requirement	-	-	-	-
	PC32. answer questions politely, with clarity and confidence, during recruitment and selection	-	-	-	-
	PC33. identify apprenticeship opportunities and register for it as per guidelines and requirements	-	-	-	-
	Total Marks	**30**	**50**	**-**	**20**
Grand Total		**170**	**280**	**-**	**100**

Annexure 7: Assessment Strategy

This section includes the processes involved in identifying, gathering, and interpreting information to evaluate the Candidate on the required competencies of the program.

For the Schemes offered on SIDH, batches are created on the SIDH portal by the TP/TC; assessment requests are made through SIDH portal. For Off-SID schemes, assessment requests are received electronically and/or through SSM (State Skill Mission) portals. If it is not a Scheme offered on SIDH or offered on SSM, then assessments requests are made via email.

Upon receiving the request, the batches are aligned for assessments to the Assessment Agency basis the assessment readiness for that particular job role/Qualification, Nano credential/Micro-credential/Standalone NOS.

Following this, an email is sent out to the TP/TC to get the confirmation on the assessment date looping IT-ITeS SSC. Once the confirmation is received, the Assessment Agency assigns a TOA certified assessor or the Proctor for conducting/facilitating the assessments as the case may be. The details of the candidates are verified and recorded at the assessment location for future reference.

QA mechanism is implemented ensuring undertaking from the TC, regular feedback is collected from the TP/TC, geo-tagged photographs of the assessment location and PC wise result analysis to enhance the quality of the assessment blueprint and assessment process thereof.

Testing Environment:

This entire process related to the testing environment is managed by the Assessment Agency in conjunction with the guidelines from NCVET.

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/Qualification, Nano credential/Micro- credential/Standalone NOS. We publish a sample question papers on our website for all stakeholders. The quality of the item bank created by the assessment designer is validated by a minimum of 2 reviewers on the following parameters:

Appropriateness of the question bank in terms of facts, data and information requited w.r.t the outcome of the Performance Criteria.

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.

Types of evidence or evidence-gathering protocol:

The time stamped and geotagged photographs of the assessment locations are collected by Proctor/Assessor during the assessment process.

Method of verification or validation:

Monitoring of batches is done as per the due process. Surprise visits are conducted at TC location during the training and assessments.

Method for assessment documentation, archiving, and access.

All assessments conducted by IT-ITeS SSC/NASSCOM, excluding those for schools, are conducted online (browser-based tests with face-to-face proctoring/online proctoring/remote auto proctoring).IT-ITeS SSC/NASSCOM stores the digital repository of the attendance sheets, photographs of assessment centres, result sheets for all assessments except school assessments which are usually available in hard copies along with all relevant artifacts.

Annexure 8: Acronym and Glossary

Acronym

Acronym	Description
AA	Assessment Agency
AB	Awarding Body
ISCO	International Standard Classification of Occupations
NCO	National Classification of Occupations
NCrF	National Credit Framework
NOS	National Occupational Standard(s)
NQR	National Qualification Register
NSQF	National Skills Qualifications Framework
OJT	On the Job Training
NASSCOM	National Association of Software and Service Companies
IT-ITeS	Information Technology and Information Technology Enabled Services
IAM	Identity and Access Management
RBAC	Role-Based Access Control
ABAC	Attribute-Based Access Control
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
SLA	Service Level Agreement
KPI	Key Performance Indicator
TCO	Total Cost of Ownership
RAID	Risks, Assumptions, Issues, and Dependencies
SOP	Standard Operating Procedure
CI/CD	Continuous Integration / Continuous Deployment
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
SOC	System and Organization Controls
MFA	Multi-Factor Authentication
PwD	Persons with Disabilities
AI/ML	Artificial Intelligence / Machine Learning
AIOps	Artificial Intelligence for IT Operations

Glossary

Term	Description
National Occupational Standards (NOS)	NOS define the measurable performance outcomes required from an individual engaged in a particular task. They list down what an individual performing that task should know and also do.
Qualification	A formal outcome of an assessment and validation process which is obtained when a competent body determines that an individual has achieved learning outcomes to given standards

Qualification File	A Qualification File is a template designed to capture necessary information of a Qualification from the perspective of NSQF compliance. The Qualification File will be normally submitted by the awarding body for the qualification.
Sector	A grouping of professional activities on the basis of their main economic function, product, service or technology.
Long Term Training	Long-term skilling means any vocational training program undertaken for a year and above. https://ncvet.gov.in/sites/default/files/NCVET.pdf