QUALIFICATION FILE

Information 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

Submitted By:

IT-ITeS Sector Skills Council NASSCOM (SSC NASSCOM)
Plot No. – 7, 8, 9 & 10
Sector – 126, Noida, Uttar Pradesh - 201303

Table of Contents

Section 1: Basic Details

1.	**Qualification Name**	**Information Security Analyst**	
2.	**Sector/s**	**IT/ITeS**	
3.	**Type of Qualification: ☐ New ☒ Revised ☐ Has Electives/Options ☐ OEM**	**NQR Code & version of the existing /previous qualification:** *QG-06-IT-01561-2023-V1.1-NASSCOM and version 3*	**Qualification Name of the existing/previous version: Information Security Specialist**
4.	**a. OEM Name** **b. Qualification Name** *(Wherever applicable)*	**Information Security Analyst**	
5.	**National Qualification Register (NQR) Code &Version** (*Will be issued after NSQC approval*)	***QG-06-IT-045892025-V2-NASSCOM and version 4***	**6. NCrF/NSQF Level:6**
7.	**Award (Certificate/Diploma/Advance Diploma/ Any Other** *(Wherever applicable specify multiple entry/exits also & provide details in annexure)*	Certificate	
8.	**Brief Description of the Qualification**	Information Security Analyst serves as a vital defender of an organization's information systems, using a combination of technical skills, knowledge of compliance frameworks, risk management practices, and effective communication to protect data integrity and support the organization's overall security posture. They are instrumental in implementing continuous monitoring mechanisms to manage risks and guide compliance strategies, ensuring that the organization adheres to relevant security policies and regulations.	

<table>
<tr><td>9.</td><td>Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee</td><td colspan="2">a. Entry Qualification & Relevant Experience:
*Relevant Experience in job roles related to IT/Computer Science/Cybersecurity
The relevant experience would include work, internship and apprenticeship after completing relevant educational qualifications.
** PG or 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 4th year UG**</td><td>-</td></tr>
<tr><td>2</td><td>Completed 3-Year UG** Degree</td><td>1.5 years of relevant experience*</td></tr>
<tr><td>3</td><td>Previous Relevant qualification of NSQF level 5.5</td><td>1.5 years of relevant experience*</td></tr>
<tr><td>4</td><td>Previous Relevant qualification of NSQF level 5</td><td>3 years of relevant experience*</td></tr>
</table>
b. Age: NA</td></tr>
<tr><td>10.</td><td>Credits Assigned to this Qualification, Subject to Assessment (as per National Credit Framework (NCrF))</td><td>19 Credits</td><td>11. Common Cost Norm Category (I/II/III)
(wherever applicable): II</td></tr>
<tr><td>12.</td><td>Any Licensing Requirements for Undertaking Training on This Qualification (wherever applicable)</td><td colspan="2">NA</td></tr>
<tr><td>13.</td><td>Training Duration by Modes of Training Delivery (Specify Total Duration as per selected training delivery modes and as per requirement of the qualification)</td><td colspan="2">☐ Offline Only ☐ Online Only ☒ Blended

<table>
<tr><th>Training Delivery Mode</th><th>Theory (Hours)</th><th>Practical (Hours)</th><th>OJT (Mandatory) Hours</th><th>OJT (Recommended) Hours</th><th>Total (Hours)</th></tr>
<tr><td>Classroom (offline)</td><td>180</td><td>270</td><td>120</td><td></td><td>570</td></tr>
<tr><td>Online</td><td>180</td><td>270</td><td>120</td><td></td><td>570</td></tr>
</table>
(Refer Blended Learning Annexure for details)</td></tr>
</table>

14.	**Aligned to NCO/ISCO Code/s** *(if no code is available mention the same)*	NCO-2015/ NIL	
15.	**Progression Path After Attaining the Qualification, wherever applicable** *(Please show Professional and Academic progression)*	This entry should refer to one or more of the following: **Professional progression**: Access to related qualification(s) at the next NSQF level – SOC Specialist, Chief Information Officer, Chief Information Security Officer, etc. **Academic progression**: Access to other qualifications at the same NSQF level - Senior Consultant Network Security, Architect Application Security, Security Operations Centre Specialist, Forensics Specialist, etc.	
16.	**Other Indian languages in which the Qualification & Model Curriculum are being submitted**	Hindi	
17.	**Is similar Qualification(s) available on NQR-if yes, justification for this qualification**	**☐ Yes ☒ No URLs of similar Qualifications:**	
18.	**Is the Job Amenable to Persons with Disability**	**☐ Yes ☒ No** **If "Yes", specify applicable type of Disability:**	
19.	**How participation of women will be encouraged?**	The Program is gender neutral although to increase the women 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, DGT/VSQ/N0102:** Employability Skills (60 Hours)	
21.	**Is Qualification suitable to be offered in Schools/Colleges**	**Schools: ☐ Yes ☒ No Colleges ☒ Yes ☐ No**	
22.	**Name and Contact Details Submitting / Awarding Body SPOC** *(In case of CS or MS, provide details of both Lead AB & Supporting ABs)*	**Name: Namrata Kapur** **Email: Standards@nasscom.in** **Contact No.: 0120-4990111** **Website: https://www.sscnasscom.com/**	
23.	**Final Approval Date by NSQC: 07th October 2025**	**24. Validity Duration: 3 Years**	**25. Next Review Date:07th October 2028**

Section 2: Module Summary

NOS/s of Qualifications

(In exceptional cases these could be described as components)

Mandatory NOS/s:

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

Th.-Theory **Pr.**-Practical **OJT**-On the Job training **Man.**-Mandatory Training **Rec.**-Recommended **Proj.-** Project

S. No	NOS/Module Name	NOS/Module Code & Version *(if applicable)*	Core/ Non-Core	NCrF/NSQF Level	Credits as per NCrF	Training Duration (Hours)					Assessment Marks					
						Th.	Pr.	OJT-Man.	OJT-Rec.	Total	Th.	Pr.	Proj.	Viva	Total	Weightage (%) (if applicable)
1.	Develop and enhance cybersecurity infrastructure	SSC/N0939, V3.0	Core	6	05	46:00	84:00	20:00	00:00	150:00	30	50	-	20	100	15%
2.	Identify and report compliance issues with respect to cybersecurity	SSC/N0917, V3.0	Core	6	02	20:00	20:00	20:00	00:00	60:00	30	50	-	20	100	15%
3.	Maintain compliance to information security policies, regulations and standards and	SSC/N0918, V3.0	Core	6	04	40:00	50:00	30:00	00:00	120:00	30	50	-	20	100	15%

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)
	address risk issues															
4.	Monitor and report on the performance of operational and technical cybersecurity measures	SSC/N0933, V3.0	Core	6	04	39:00	61:00	20:00	00:00	120:00	30	50	-	20	100	15%
5.	Foster collaboration between various stakeholders to ensure cohesive cybersecurity practices across the organization.	SSC/N0927, V3.0	Core	6	01	06:00	09:00	15:00	00:00	30:00	30	50	-	20	100	15%
6.	Make reports based on test results and making enhancements to existing security solutions	SSC/N0936, V3.0	Core	6	01	05:00	10:00	15:00	00:00	30:00	30	50	-	20	100	15%

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)
7.	Employability Skills (60 Hours)	DGT/VSQ/N0102, V1.0	Non-Core	4	02	24:00	36:00	00:00	00:00	60:00	20	30	-	-	50	10%
Duration (in Hours)/Total Marks					19	180:00	270:00	120:00	00:00	570:00	200	330	-	120	650	100%

Elective NOS/s:

S. No	NOS/Module Name	NOS/Module Code & Version *(if applicable)*	Core/ Non-Core	NCrF/NSQF Level	Credits as per NCrF	Training Duration (Hours)					Assessment Marks					
						Th.	Pr.	OJT-Man.	OJT-Rec.	Total	Th.	Pr.	Proj.	Viva	Total	Weightage (%) *(if applicable)*
1.																
2.																
Duration (in Hours) / Total Marks																

Optional NOS/s:

S. No	NOS/Module Name	NOS/Module Code & Version *(if applicable)*	Core/ Non-Core	NCrF/NSQF Level	Credits as per NCrF	Training Duration (Hours)					Assessment Marks					
						Th.	Pr.	OJT-Man.	OJT-Rec.	Total	Th.	Pr.	Proj.	Viva	Total	Weightage (%) *(if applicable)*
1.																
2.																
Duration (in Hours) / Total Marks																

Assessment - Minimum Qualifying Percentage

Assessment - Minimum Qualifying Percentage
Minimum Pass Percentage – Aggregate at qualification level: 70 % (Every Trainee should score specified minimum aggregate passing percentage at qualification level to successfully clear the assessment.)

Section 3: Training Related

1.	**Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	**Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science) **Industry & training experience:** 2 years of industry experience in Cybersecurity. The industry experience would include work, internship, and apprenticeship undertaken after regular graduation **Certification:** "Trainer" mapped to the Qualification Pack "MEP/Q2601" Minimum accepted score is 80% aggregate
2.	**Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	**Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science) **Industry & training experience:** 4 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **Certification:** "Master Trainer" mapped to the Qualification Pack "MEP/Q2602" Minimum accepted score is 90% aggregate
3.	**Tools and Equipment Required for the Training**	☒Yes ☐No *(If "Yes", details to be provided in Annexure)*
4.	**In Case of Revised Qualification, details of Any Upskilling Required for Trainer**	NA

Section 4: Assessment Related

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	**Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science)

		Industry & Training Experience: 2 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **Certification:** "Assessor" mapped to the Qualification Pack "MEP/Q2701" Minimum accepted score is 80% aggregate.
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines), (wherever applicable)*	**Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science) **Industry & Training Experience:** 2 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **Certification:** "Assessor" mapped to the Qualification Pack "MEP/Q2701" Minimum accepted score is 80% aggregate.
3.	**Lead Assessor's/Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	**Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science) **Industry & Training Experience:** 4 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **Certification:** "Lead Assessor" mapped to the Qualification Pack "MEP/Q2702" Minimum accepted score is 90% aggregate.
4.	**Assessment Mode** *(Specify the assessment mode)*	The assessment will consist of a blend of hands-on practical evaluations, viva-voce, and online proctored scenario-based multiple-choice questions ensuring a thorough evaluation of the individual's proficiency in learning outcomes, practical understanding, and real-world application of concepts.
5.	**Tools and Equipment Required for Assessment**	☒ Same as for training ☐ Yes ☐ No *(details to be provided in Annexure-if it is different for Assessment)*

Section 5: Evidence of the Need for the Qualification

Provide Annexure/Supporting documents name.

1.	Latest Skill Gap study (not older than 2 years) (Yes/No): Yes
2.	Latest Market Research Reports or any other source (not older than 2 years) (Yes/No): Yes
3.	Government/Industry initiatives/requirement (Yes/No): Industry Initiatives
4.	Number of industry validations provided: 21

5.	Estimated number of people to be trained and employed: NA
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_SSCQ0923_Information Security Analyst_V4
9.	**Supporting Document:** Career Progression *(Mandatory-Public View)*	Occupational Map-Cybersecurity
10.	**Supporting Document:** Occupational Map *(Mandatory)*	Occupational Map-Cybersecurity
11.	**Supporting Document:** Assessment SOP *(Mandatory)*	NA
12.	**Any Other document you wish to submit:**	NA

Annexure: Evidence of Level

NCrF/NSQF Level Descriptors	Key requirements of the job role/ outcome of the qualification	How the job role/ outcomes relate to the NCrF/NSQF level descriptor	NCrF/NSQF Level
Professional Theoretical Knowledge/Process	**Define the cyber security infrastructure policy or technical security policy for an organization** • Research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities, and security risks • gather sufficient accurate information on which to determine potential costs, benefits, and effectiveness of recommended security solutions • review the usage of existing cyber security infrastructure and assess risks w.r.t security objectives • create a map of the security counter measures at different layers: network security, access control mechanisms, endpoint security, application security, databases, and unstructured data • identify and prioritize critical business functions in collaboration with organizational stakeholders **Monitor and report on performance of operational and technical cyber security measures** • implement automated solutions for monitoring and reporting on the implementation and functioning of	Evaluation of assets, threats, vulnerabilities, and security risks, creating a map of the security counter measures at different layers, and administering the functioning of cyber security infrastructure components in various scenarios and security situations requires the job holder to obtain specialised theoretical and practical skills, in a wide range of IT infrastructural contexts. Deploying a dynamic network topology application system to automatically map and update the infrastructure components upon scaling systems and information, means to readily prepare for all routine and non-routine test case scenarios in maintaining IT infrastructure.	6

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
	cyber security infrastructure components • assess the configurations against policy and approved baseline configurations using automated tools • identify uncommon traffic trends and false positives • obtain vulnerabilities identification and analysis, risk assessment reports, infrastructure security key performance indicators from authorised sources **Configure cyber security infrastructure components** • protect the network device configuration file from unauthorized disclosure • use a dynamic network topology application to map infrastructure initially and to update the map automatically on adding machines and entering the data • implement safeguards through software to protect end-user machines against attacks • test the configurations and the secure values or parameters in virtual		

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
	environment and resolve issues and deviations identified during testing • implement baseline configurations in a centralized and automated manner using automated configuration management tools, automated scripts, vendor-provided mechanisms, etc. **Maintain and enhance cyber security infrastructure components** • conduct functional and connectivity testing to ensure continuing operability • maintain baseline system security according to organizational policies • analyse TCP traffic and update atomic signatures to reduce resource consumption • install server updates and enhancements • implement new system design procedures, test procedures, and quality standards • plan and coordinate the installation of new or modified hardware, operating systems, and baseline software		
Professional and Technical Skills/ Expertise/ Professional Knowledge	• cyber security architecture concepts, including topology, protocols, components, and principles (e.g., application of defence-in-depth)	Defining security infrastructure policies, process controls and standards for an enterprise requires a thorough understanding of the business priorities, existing IdAM technologies, risks faced by the	6

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
	• relevant networking concepts, devices, and terminologies • computer network defence (CND) and vulnerability assessment tools, including open-source tools, and their limitations, compatibilities, and capabilities • information assurance (IA) principles • information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption) • awareness of Security Modelling technique • awareness of Virtualization techniques and Container services • network traffic analysis methods • network design processes, to include understanding of security objectives, operational objectives, and trade-offs • organization's Local Area Network (LAN)/Wide Area Network (WAN) pathways • capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware	organisation, security requirements, organisational structure, etc. To standardize security operations requires the job role holder to be factually correct and have a wide-ranging specialised theoretical skills.	
Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	• plan for remedial action or counter measures for areas where inconsistencies have been identified	Developing remedial action plans and counter measures to maintain consistent operations of enterprise infrastructure and preparing recommendations that have the potential to meet	6

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
	• recognise the roles, responsibilities, interests, and concerns of the stakeholders in other business functions • discuss and consult with stakeholders from other functions in relation to key decisions and activities impacting them • monitor and review the effectiveness of working relationships with stakeholders in other business functions, seeking and providing feedback, in order to identify areas for improvement • ensure the allocation and authorisation of work to the project management team is consistent with achieving the project objectives • identify and determine the cost, potential benefits, and effectiveness of recommended security solutions, based on valid assumptions, considerations, and information, including possible constraints • prepare recommendations that have the potential to meet the security objectives of the organisation • ensure technology risk considerations are identified and adequately addressed for new application developments, integration, and deployment	the security objectives of the organisation, require the job holder to be highly cognitive and practical in approach	

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
Broad Learning Outcomes/Core Skill	• provide the organisation with considered advice on the implications of accepting, modifying, or rejecting security recommendations • consult with engineering teams in various cyber security functions for their evaluation and recommendation regarding existing security infrastructure • provide input to the Risk Management Framework (RMF) process activities and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials) • ensure the allocation and authorisation of work to the project management team is consistent with achieving the project objectives • Implement automated solutions and manual processes for monitoring and reporting on the functioning and performance of cyber security infrastructure components • assess the configurations against policy and approved baseline configurations using automated tools • reconcile changes detected as a result of monitoring activities with approved changes	The job role holder needs to write automation scripts, conduct vulnerability assessments, configure infrastructure components, analyse network traffic, conduct technical risk analysis, cost modelling and business impact analysis on a daily basis. This would require the job holder to have a strong hold in logical, mathematical, and analytical skills. Security Infrastructure Specialists also need to work in collaboration with various stakeholders ranging from Business heads to Security teams, network engineers, system admins, vendors, specialists. This requires a person with extremely good data organization and presentation, communication, and interpersonal skills.	6

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
	• analyse the results of monitoring activities to determine the reason(s) that an unauthorized change occurred • conduct periodic server maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing • implement new system design procedures, test procedures, and quality standards • repair network connectivity problems • follow configuration change control process in case and change of configuration is required during maintenance or troubleshooting		
Responsibility	• Responsibility of his own work and also responsible for others work and learning	There will be teams involved in the various technical functions that support the forensic specialist, however, complete responsibility lies with the forensic specialist.	6

Annexure: Tools and Equipment (lab set-up)

List of Tools and Equipment

Batch Size:

S. No.	Tool / Equipment Name	Specification	Quantity for specified Batch size
1	PC/Laptop with internet	-	
2	Network Protocol analyser	Wireshark	
3	Penetration Testing Framework	Metasploit community edition	
4	Intrusion Detection System	Snort	

5	Antivirus software	ClamAV	
6	Vulnerability Scanning Tool	OpenVAS	
7	Log Analysis and Management Tool	ELK Stack	
8	Risk Assessment Tool	OpenSCAP	
9	Compliance Management Platform	OpenGRC	
10	Web Application Scanner	OWASP ZAP	
11	Intrusion Detection/Monitoring Tool	Security Onion	
12	Virtual Lab Environment	Vulnhub	

*Open Source Tools

Classroom Aids

The aids required to conduct sessions in the classroom are:

1. White Board
2. White Board Marker
3. Projector

Annexure: Industry Validations Summary

Provide summary information of all the industry validation in table. This is not required for OEM Qualifications.

S. No	Organization Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID	LinkedIn Profile (if available)

1	Renew	Aseem Mukhi	Chief Information Security Officer	-	9990002658	assem.mukhi@gmail.com	https://www.linkedin.com/in/aseem-mukhi-1544854/
2	Sankey Solutions	Sobha Patil	CEO	-	9008193344	shobha@sankeysolutions.com	https://www.linkedin.com/in/shobhapatil/?originalSubdomain=in
3	Accolite Digital	Ayushmaan Pandey	Senior Software Engineer	-	8077386365	ayushmaan.pandey@accolitedigital.com	https://www.linkedin.com/in/ayushmaanpandey
4	Infosys	Vivek Pilaniya	Program Manager	-	9718423687	vivek.pilania@infosys.com	https://www.linkedin.com/in/vivekpilania-iimc
5	Data Switch	Thilak Hari A	Product Engineer	-	6393798750	thilakhariharan@gmail.com	https://www.linkedin.com/in/thilak-hariharasudhan-43a89b269/
6	Forbes	Naveenkumar Janakiraman	Data Research Analyst	-	9976773109	naveenkumarj4997@gmail.com	https://www.linkedin.com/in/naveenkumar-janakiraman
7	S3V Vascular Technologies	Yeaswanth Raj V	Clinical Research Executive	-	7502629955	yeaswanthraj@gmail.com	-
8	Kornferry	Ragul Kumar	Data analyst	-	9659964881	ragul@kornferry.com	https://www.linkedin.com/in/ragul-kumar-b2297a171/
9	Acolyte	Saranya	Research Analyst	-	9944313170	saranyakathir128@gmail.com	-
10	Frontier	Santhosh kumar S	DevOps L1	-	9655747400	santhoshselvaraj24031998@gmail.com	-
11	Amazon	Asvin Ragav R	Data Associate	-	9994308478	asvinragav16@gmail.com	-
12	Rndsoft	Tamilselvan	Software developer	-	9361784871	dtamilselvan1004@gmail.com	-
13	Intellibren	Kailash PD	Director	-	6374700185	kailash@intellibren.com	-

14	Mindshare (Inclusive Minds)	Pamindar Singh	Team Lead	-	8713901984	paminder.singh@themindshare.in	https://www.linkedin.com/in/paminder-singh-7990b8101/
15	Iaccept software pvt ltd	B Mohan Kumar	Founder	-	9845208784	mohan@iaccept.in	https://www.linkedin.com/in/bmohankumar/?originalSubdomain=in
16	QAcadmey	Deepak Gour	Product and Academic Head	-	9893554394	deepak@qacademy.ca	https://ca.linkedin.com/in/deepak-gour-8853968
17	TCS	Karthiga N	Test Analyst	-	7092257551	karthiga0115@gmail.com	-
18	Skillsda	Sankar Vijyan/Thiru R	Centre Manager/Head R&D	-	9894801793	sv@skillsda.com/thiru@skillsda.com	https://www.linkedin.com/in/sankar-vijayan-73a33852/
19	Wipro	Narendra Nande	Director	-	9900086708	narendra.nande@wipro.com	https://www.linkedin.com/in/narendra-nande-84402a2/?originalSubdomain=in
20	Barq	Satheesh Sekar	Senior Decision Scientist	-	9444218513	satheeshk.sekar@gmail.com	https://www.linkedin.com/in/satheeshksekar/?originalSubdomain=in
21	Neoquant	Rishi Agrawal	Chief Technology Officer	-	7702191049	agrishi@gmail.com/Rishi.agarwal@neoquant.com	https://www.linkedin.com/in/agrishi/?originalSubdomain=in

Annexure: Training & Employment Details

Training & Employment Projections:

Year	Total Candidates		Women		People with Disability	
	Estimated Training #	Estimated Employed Opportunities	Estimated Training #	Estimated Employed Opportunities	Estimated Training #	Estimated Employed Opportunities

Data to be provided year-wise for next 3 years.

Training, Assessment, Certification, and Placement Data for previous versions of qualifications:

Qualification Version	Year	Total Candidates			Women			People with disability		
		Trained	Assessed	Certified	Trained	Assessed	Certified	Trained	Assessed	Certified

Applicable for revised qualifications only; data to be provided year-wise for the next 3 years.

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

1.

Content availability for the previous version of qualifications:

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

Language in which content is available:

Annexure: Blended Learning

Blended Learning Estimated Ratio & Recommended Tools:

Refer NCVET "Guidelines for Blended Learning for Vocational Education, Training & Skilling" available on:
https://ncvet.gov.in/sites/default/files/Guidelines%20for%20Blended%20Learning%20for%20Vocational%20Education,%20Training%20&%20Skilling.pdf

S. No.	Select the Components of the Qualification	List Recommended Tools – for all Selected Components	Offline: Online Ratio
1	☐Theory/ Lectures - Imparting theoretical and conceptual knowledge	NA	NA
2	☐Imparting Soft Skills, Life Skills, and Employability Skills /Mentorship to Learners	NA	NA
3	☐Showing Practical Demonstrations to the learners	NA	NA
4	☐Imparting Practical Hands-on Skills/ Lab Work/ workshop/ shop floor training	NA	NA
5	☐Tutorials/ Assignments/ Drill/ Practice	NA	NA
6	☐Proctored Monitoring/ Assessment/ Evaluation/ Examinations	NA	NA

7	☐On the Job Training (OJT)/ Project Work Internship/ Candidate Training	NA	NA

Annexure: Detailed Assessment Criteria

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

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
SSC/N0939 (Develop and enhance cybersecurity infrastructure)	PC1. Assess existing cybersecurity infrastructure by reviewing current security measures consulting with engineering teams and understanding the security objectives and risks	3	5	-	2
	PC2. Create a security layer map covering network access control endpoint application and data security to identify protection gaps and prioritize critical functions	3	5	-	2
	PC3. Evaluate the organization's security posture and infrastructure capability to address potential threats considering organizational needs and acceptable risk levels	3	5	-	2
	PC4. Develop a comprehensive cybersecurity architecture plan including policies scope and technical specifications ensuring alignment with business continuity and disaster recovery plans	3	5	-	2
	PC5. Implement baseline configurations and security controls using automated configuration management and patch management tools to maintain operational integrity	3	5	-	2
	PC6. Test the functionality and connectivity of security components monitor infrastructure for vulnerabilities and adjust measures based on emerging threats	3	5	-	2
	PC7. Draft and enforce security policies incident response plans and maintain the confidentiality and security of security-related information	3	5	-	2
	PC8. Provide ongoing training conduct regular compliance assessments and review third-party security relationships to ensure continuous security improvement	3	5	-	2

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC9. Define key performance indicators and establish reporting mechanisms for cybersecurity effectiveness incorporating feedback from incidents and audits	3	5	-	2
	PC10. Maintain detailed documentation of infrastructure design configurations and incident response processes to ensure transparency and continual enhancement	3	5	-	2
	Total Marks	**30**	**50**	**-**	**20**
SSC/N0917 (Identify and report compliance issues with respect to cybersecurity)	PC1. Receive and interpret organizational policies, contractual requirements, and legislative requirements related to cybersecurity from authorized sources.	1	3	-	1
	PC2. Gather relevant information about the asset or process under review and identify necessary supporting resources (platforms, operating systems, personnel).	1	3	-	1
	PC3. Develop a compliance checklist with stakeholder input, detailing requirements, controls, potential threats, probability of occurrence, and potential impact.	2	3	-	1
	PC4. Obtain authorization to access data and evaluate processes and operations from relevant authorities, ensuring lawful conduct.	2	3	-	1
	PC5. Collect and store necessary evidence to support compliance assessments and audits.	2	3	-	1
	PC6. Evaluate processes and documentation for non-conformance to policies, procedures, standards, and controls as identified in the compliance checklist.	2	3	-	1
	PC7. Assess and validate a system's compliance with IT security, resilience, and dependability requirements.	2	3	-	1
	PC8. Conduct security authorization reviews and assurance case developments for the initial installation of software applications, systems, and networks to confirm acceptable risk levels.	2	3	-	1
	PC9. Verify that accreditation and assurance documentation for software applications, networks, and systems is current, with implemented security postures.	2	3	-	1
	PC10. Inspect continuous monitoring results to ensure risk levels remain within acceptable limits for applications, networks, or systems.	2	3	-	1
	PC11. Identify and assess exposure to risks, threats, and legal/compliance regulations as outlined in the compliance checklist.	2	3	-	1
	PC12. Document deviations from compliance standards and recommend corrective actions, ensuring accountability.	2	3	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC13. Provide a comprehensive technical evaluation of software applications, systems, or networks, documenting security posture, capabilities, and vulnerabilities against confidentiality, integrity, and availability (CIA) compliance.	2	3	-	2
	PC14. Prepare compliance audit and analysis reports for various stakeholders, ensuring clarity and actionable insights.	2	3	-	2
	PC15. Complete assigned tasks and activities per defined standards and timelines, ensuring successful execution.	2	4	-	2
	PC16. Develop and maintain reporting dashboards that align with organizational requirements and schedules.	2	4	-	2
	Total Marks	**30**	**50**	**-**	**20**
SSC/N0918 (Maintain compliance to information security policies, regulations and standards and address risk issues)	PC1. Communicate compliance audit and risk assessment results to relevant personnel.	2	3	-	1
	PC2. Identify and share compliance issues found during audits with appropriate personnel.	2	3	-	1
	PC3. Plan and coordinate organizational activities to ensure compliance with regulations and standards.	2	3	-	1
	PC4. Document and implement all policies and procedures effectively.	2	3	-	1
	PC5. Conduct internal reviews to identify compliance issues and initiate corrective actions.	2	4	-	2
	PC6. Submit compliance reports to regulatory bodies.	2	4	-	2
	PC7. Monitor risk factors in organizational operations and take necessary corrective actions.	3	5	-	2
	PC8. Present identified compliance issues to management for prioritization and risk mitigation.	3	5	-	2
	PC9. Maintain regular communication with various stakeholders to coordinate compliance activities.	3	5	-	2
	PC10. Document all processes and outcomes for audits.	3	5	-	2
	PC11. Utilize AI-driven tools for continuous monitoring of compliance and risk assessment.	3	5	-	2
	PC12. Implement cloud-based compliance management solutions to streamline reporting and documentation.	3	5	-	2

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	Total Marks	**30**	**50**	**-**	**20**
SSC/N0933 (Monitor and report on the performance of operational and technical cybersecurity measures)	PC1. Implement automated solutions to monitor and report the status and performance of cybersecurity infrastructure components and document any systems not covered by automation	3	5	-	2
	PC2. Develop manual processes for monitoring and reporting on cybersecurity measures to ensure comprehensive coverage and compliance	3	5	-	2
	PC3. Collect and analyze data on the implementation and effectiveness of operational and technical cybersecurity controls using both automated tools and manual methods	3	5	-	2
	PC4. Assess configurations against policy standards and baseline configurations and facilitate reporting for management and compliance through security information and event management systems	3	5	-	2
	PC5. Identify unusual traffic patterns and false positives reconcile detected changes with authorized change control records and analyze unauthorized changes to determine their causes	3	5	-	2
	PC6. Obtain and review vulnerability risk assessment and cybersecurity audit reports from authorized sources to inform monitoring activities and decision-making	3	5	-	2
	PC7. Select key metrics and analyze infrastructure security key performance indicators to measure the effectiveness and efficiency of cybersecurity measures	3	5	-	2
	PC8. Consolidate findings into detailed reports to support management decisions compliance requirements and improvement initiatives	3	5	-	2
	PC9. Plan and implement remedial actions for identified inconsistencies or vulnerabilities detected during monitoring activities using automated tools	3	5	-	2
	PC10. Ensure all updates and changes to supporting documentation are made after proper authorization to maintain accurate records and compliance	3	5	-	2
	Total Marks	**30**	**50**	**-**	**20**
SSC/N0927(Foster collaboration between various stakeholders to ensure cohesive	PC1. Identify key stakeholders and understand their roles and concerns in relation to cybersecurity.	3	5	-	2
	PC2. Create an inventory of cybersecurity-related operations and responsibilities.	3	5	-	2
	PC3. Collaborate with stakeholders to discuss key decisions impacting cybersecurity practices.	3	5	-	2

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
cybersecurity practices across the organization)	PC4. Track and follow up on actionable items agreed upon with stakeholders.	3	5	-	2
	PC5. Monitor the effectiveness of interdepartmental relationships and seek feedback for improvement.	3	6	-	2
	PC6. Address conflicts of interest with stakeholders in a manner that minimizes disruption.	3	6	-	2
	PC7. Ensure agreements are fulfilled and communicate any potential difficulties promptly.	4	6	-	2
	PC8. Promote awareness of AI and cloud technologies among stakeholders regarding their impact on cybersecurity.	4	6	-	3
	PC9. Collaborate with cloud service providers to ensure compliance with established security standards.	4	6	-	3
	Total Marks	**30**	**50**	**-**	**20**
SSC/N0936 (Make reports based on test results and make enhancements to existing security solutions)	PC1. Document the timeline and details of attacks including logs security vulnerabilities and measures taken for reconnaissance and footprinting activities	3	5	-	2
	PC2. Use the latest risk assessment tools to analyze test results and inform report content and security improvements	3	5	-	2
	PC3. Identify and report sources of threats and potential weaknesses in the network to guide mitigation strategies	3	5	-	2
	PC4. Update initial testing reports into comprehensive final reports tailored to the target audience with appropriate style and format	3	5	-	2
	PC5. Organize and classify information within reports according to the organization's information classification policies for clarity and security	3	5	-	2
	PC6. Generate separate detailed reports on issues such as misconfigured DNS servers attack logs and identified vulnerabilities for future reference	3	5	-	2
	PC7. Integrate attack phase logs to provide a comprehensive overview of threats and their severity levels in a standardized format	3	5	-	2
	PC8. Record weaknesses in the system to support ongoing threat management governance and future security planning	3	5	-	2
	PC9. Recommend controls solutions architectural changes and security hardening measures for servers and network devices to prevent future exploits	3	5	-	2

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC10. Enhance existing security tools such as firewalls IDS patch management systems and testing tools to improve security posture and efficiency	3	5	-	2
	Total Marks	**30**	**50**	**-**	**20**
DGT/VSQ/N0102 Employability Skills (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 Apprenticeships & Jobs	2	3	-	-
	Total Marks	**20**	**30**	**-**	**-**
Grand Total Marks		**200**	**330**	**-**	**120**

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.