QUALIFICATION FILE

IoT 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) ☒ FutureSkills ☐ 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**	**IoT 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-05-IT-01565-2023-V1.1-NASSCOM & Version 3	**Qualification Name of the existing/previous version:** IoT Security Specialist
4.	**a. OEM Name** **b. Qualification Name** *(Wherever applicable)*		
5.	**National Qualification Register (NQR) Code &Version** (*Will be issued after NSQC approval*)	QG-06-IT-045982025-V2-NASSCOM & 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**	An IoT Security Analyst is a professional specializing in protecting Internet of Things (IoT) devices, networks, and systems from threats and vulnerabilities. They design, implement, manage, and monitor security measures tailored to IoT environments, ensuring the confidentiality, integrity, and availability of data and operations. Their role involves understanding the unique security challenges of IoT devices—such as limited processing power, diverse protocols, and widespread deployment—and applying best practices, standards, and open-source tools to safeguard these assets. They also conduct vulnerability assessments, develop incident response plans, and ensure compliance with relevant security standards. Overall, an IoT Security Specialist helps organizations maintain resilient and secure IoT ecosystems critical for modern businesses and infrastructure.	
9.	**Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee**	**Entry Qualification & Relevant Experience:** *Relevant Experience in job roles related to Computer Science/IT/Network Security/Cybersecurity/IoT The relevant experience would include work, internship, and apprenticeship after completing relevant educational qualifications. * PHD or PG or UG or diploma with courses related to Engg./ Science	

		S. No. / **Academic/Skill Qualification (with Specialization - if applicable)** / **Required Experience (with Specialization - if applicable)** 1 / Completed 4 Year UG* / - 2 / Completed 3-Year UG* Degree / 1.5 years of relevant experience** 3 / Previous Relevant qualification of NSQF level 5.5 / 1.5 years of relevant experience** **Min Age:** NA
10.	**Credits Assigned to this Qualification, Subject to Assessment** *(as per National Credit Framework (NCrF))*	19 Credits **11. Common Cost Norm Category (I/II/III)** *(wherever applicable)*: **II**
12.	**Any Licensing Requirements for Undertaking Training on This Qualification** *(wherever applicable)*	NA
13.	**Training Duration by Modes of Training Delivery** *(Specify **Total Duration** as per selected training delivery modes and as per requirement of the qualification)*	☐**Offline Only** ☐ **Online Only** ☒ **Blended** **Training Delivery Mode** / **Theory (Hours)** / **Practical (Hours)** / **OJT (Mandatory) Hours** / **OJT (Recommended) Hours** / **Total (Hours)** **Classroom (offline)** / 168 / 282 / 120 / - / 570 **Online** / 168 / 282 / 120 / - *(Refer Blended Learning Annexure for details)*
14.	**Aligned to NCO/ISCO Code/s** *(if no code is available mention the same)*	NCO- 2015/2522.0201
15.	**Progression Path After Attaining the Qualification, wherever applicable** *(Please show Professional and Academic progression)*	This entry should refer to one or more of the following: **Professional progression**: access to related qualification(s) at the next NSQF level: Lead IoT Security Specialist, Lead IoT Network Specialist

		Academic progression: access to related qualification(s) at the next NSQF level: IoT Network Specialist	
16.	**Other Indian languages in which the Qualification & Model Curriculum are being submitted**	Hindi	
17.	**Is similar Qualification(s) available on NQR-if yes, justification for this qualification**	**☐ Yes ☒ No URLs of similar Qualifications:**	
18.	**Is the Job Amenable to Persons with Disability**	**☒ Yes ☐ No** **If "Yes", specify applicable type of Disability:** Visual, Hearing or Speech impairment, Locomotor Disability	
19.	**How will participation of women be encouraged?**	The Program is gender neutral although to increase women's participation, organizations are keeping aside a few seats to encourage 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 **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.	Design processes to manage security threats and incidents across multiple technology layers	SSC/N8231 V3	Core	6	05	44:00	76:00	30:00	00:00	150:00	30	50	-	20	100	17
2.	Detect occurrences of security incidents to IoT solutions	SSC/N8232 V3	Core	6	05	45:00	75:00	30:00	00:00	150:00	30	50	-	20	100	17
3.	Respond to detected security incidents and restore affected capabilities	SSC/N8233 V3	Core	6	03	30:00	45:00	15:00	00:00	90:00	30	50	-	20	100	17
4.	Create technical documents and manuals	SSC/N8238 V3	Core	5	01	05:00	10:00	15:00	00:00	30:00	30	50	-	20	100	17
5.	Operational Technology Security	SSC/N8249 ,V1	Core	6	03	20:00	40:00	30:00	00:00	90:00	30	50	-	20	100	17
6.	Employability Skills	DGT/VSQ/N0102, V1	Non - Core	4	02	24:00	36:00	00:00	00:00	60:00	20	30	-	-	50	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)
	Grand Total				**19**	**168:00**	**282:00**	**120:00**	**00:00**	**570:00**	**170**	**280**	**-**	**100**	**550**	**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

*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 (Engineering/ Technology/ Computer Science) **Industry & training experience**: 2 years of industry experience in IoT. The industry experience would include work, internship, and apprenticeships 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 IoT. 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 IoT. 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 IoT. 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 IoT. 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): NA
2.	Latest Market Research Reports or any other source (not older than 2 years) (Yes/No): NA
3.	Government/Industry initiatives/requirement (Yes/No): 15
4.	Number of industry validations provided: NA
5.	Estimated number of people to be trained and employed: 1000
6.	Evidence of Concurrence/Consultation with Line/State Departments: NA 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)*	NA
7.	**Annexure:** Acronym and Glossary *(Optional)*	NA

8.	**Supporting Document:** Model Curriculum *(Mandatory-Public View)*	MC_SSC/Q8207_IoT Security Specialist_V4
9.	**Supporting Document:** Career Progression *(Mandatory-Public View)*	NA
10.	**Supporting Document:** Occupational Map *(Mandatory)*	IT-ITeS Occupation Map
11.	**Supporting Document:** Assessment SOP *(Mandatory)*	Assessment Strategy
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
Process	**Requires a command of wide-ranging specialised theoretical and practical skills, involving variable routine and nonroutine contexts.** • Record, classify and prioritize information security incidents using standard templates and tools • Identify procedures/ guidelines/ checklists that will be used for audits • Record and document audit tasks and results using standard tools and templates • Analyse data security performance metrics for action by appropriate people • Carry out information security assessments and configuration reviews • Track progress of investigations into information security incidents • Escalate security breaches to appropriate where standards or SLAs have not been complied with • Constantly update the organization's knowledge base with information security incidents and how they were managed	The individual in this role must work in a constantly changing environment where he/she needs to designing processes to mitigate security risk at the network, hardware, cloud, application and platform layers. To perform his/her role effectively, the individual requires a vast understanding of the fundamentals of security and the various levels that they need to cover: device, cloud, communications, applications, etc. He/she needs to adapt to changing circumstances while working within the organization's processes and guidelines.	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
	• Check that your own and/or your peers' work meets customer requirements		
Professional knowledge	**Wide-ranging factual and theoretical knowledge in broad contexts within a field of work or study.** • Knowledge of the organization's information security systems and tools and how to access and maintain these • Fundamentals of security and the various levels that they need to cover: device, cloud, communications, applications, etc. • How to define processes for handling security across various solution layers • How to create and update Intrusion Detection Systems (IDS) • Knowledge of organizational policies, standards, procedures, guidelines, systems and checklists for audits and their role in applying these • How to leverage the organization's knowledge base and use this to support audits • Understanding of all the different systems that may require audit tasks including servers, storage devices, infrastructure, data assets and networks • Knowledge of features, configuration and specifications of systems and devices which may be audited • Knowledge of common audit techniques and how to record and report audit tasks	The individual in the role must have a vast amount of knowledge across organizational policies, procedures and guidelines which relate to maintaining solution security. Since this is a role that requires the application of knowledge across different changing scenarios, deep and vast knowledge is a necessity.	6
Professional skill	**Wide range of cognitive and practical skills required to generate solutions to specific problems in a field of work of study.** • Evaluate security vulnerabilities discovered for their relevance, root causes, risk criticality, and corresponding mitigation methods	The role demands a skillset that allows the individual to detect occurrences of security incidents to IoT solutions. To do so, the individual needs to have prior experience in a related field and must have the analytical ability to put these skills in practice.	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
	• Access and analyse information security performance metrics • Identify and resolve data security vulnerabilities and issues • How to define security parameters for data stored in cloud platforms, open source or in-memory databases • Develop encryption standards and access controls for data stored in cloud platforms, open source or in-memory databases • How to run routine operational procedures and tasks required to co-ordinate and respond to information security incidents		
Core skill	**Good logical and mathematical skill understanding of social political and natural environment and organising information, communication and presentation skill.** • Apply security controls in line with data policies, procedures and guidelines • Develop encryption standards and access controls for data • Conduct penetration testing using automatic scanning technologies and manual testing • Awareness of global data standards and regulations • Evaluate criticality and security threat level of each IoT asset of the organization	The individual should possess in depth knowledge of the tools required review past incidents, audit operations, security analysis, continuous monitoring and threat assessment and detection maintenance. Apart from the ability to use these tools, the individual needs to have a clear picture of the appropriate integrations that need to be achieved. To do so, he/she must have a strong understanding of different business and technological trends.	6
Responsibility	**Full responsibility for output of group and development.** • Listen effectively and orally communicate information accurately with attention to details • Check your work is complete and free from errors • Make decisions on suitable courses of action • Apply balanced judgements to different situations • Ask for clarification and advice from appropriate people • Build and maintain positive and effective relationships with clients	The role demands working in a team to deliver consistent and accurate data integrations. This may involve helping peers with their work from time to time and providing feedback and advice to help improve the quality of their work. Since this role is likely to have people reporting to it, the individual performing this role is supposed to take responsibility for the output and the development of the entire team.	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
	• Check that your own and/or your peers' work meets customer requirements • Plan and organize your own work to achieve targets and deadlines • Work with colleagues to deliver shared goals		

Annexure: Tools and Equipment (lab set-up)

Batch Size:

S. No.	Tool / Equipment Name	Specification	Quantity for the specified Batch size
1	PC/Laptop with internet	-	
2	IoT Platform	Eclipse IoT	
3	Security, Encryption and Secure Communication Tool	OpenSSL	
4	Vulnerability Assessment Tools	OpenVAS	
5	Patch and Device Management	Ansible	
6	Log Management and Analysis	ELK Stack	
7	Forensics & Evidence	Volatile Framework	
8	Threat Intelligence, Automation and monitoring	OSSEC	
9	Documentation	Libre office, Google Docs	
10	Network Design and Diagramming	Draw.io	
11	OT Asset Discovery and Scanning	Nmap	
12	Network Monitoring & Protocol Analysis	Wireshark	

*Tools are open source

Annexure: Industry Validations Summary

Provide summary information of all the industry validation in table.

S. No	Organisation Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID	LinkedIn Profile
1	Wipro	Narendra Nande	Director	-	9900086708	narendra.nande@wipro.com	https://www.linkedin.com/in/narendra-nande-84402a2/?originalSubdomain=in
2	Skillsda	Sankar Vijyan/Thiru R	Centre Manager/Head R&D	-	9894801793	sv@skillsda.com/thiru@skillsda.com thiru@skillsda.com	https://www.linkedin.com/in/sankar-vijayan-73a33852/ https://www.linkedin.com/in/dr-thirukkumaran-raman-1435a1216/
3	Forbes	Naveenkumar Janakiraman	Data Research Analyst	-	9976773109	naveenkumarj4997@gmail.com	-
4	Sankey Solutions	Chandan Rajurohit	Solution lead	-	8369853182	Chandan.r1@sankeysolutions.com	-
5	Intellibren	Kailash PD	Director	-	6374700185	Kailash@intellibren.com	-
6	Mind share	Pamindar Singh	Team Lead	-	8713901984	paminder.singh@themindshare.in	https://www.linkedin.com/in/paminder-singh-7990b8101/
7	Amazon	Asvin Ragav R	Data Associate	-	9994308478	asvinragav16@gmail.com	-
8	Data Switch	Thilak hariharaSudhan A	Product Engineer	-	6393798750	thilakhariharan@gmail.com	https://www.linkedin.com/in/thilak-hariharasudhan-43a89b269/?originalSubdomain=in
9	Q Acadmey	Deepak Gour	Product and Academic Head	-	9893554394	deepak@qacademy.ca	https://ca.linkedin.com/in/deepak-gour-8853968
10	Frontier	Santhosh kumar S	DevOps Engineer L1	-	9655747400	santhoshselvaraj24031998@gmail.com	-
11	Kornferry	Ragul	Data analyst	-	9659964881	ragulblooper143@gmail.com	-
12	Tata consultancy services	Karthiga N	Test Analyst	-	7092257551	karthiga0115@gmail.com	-

13	Accenture	Sree Karthikeyan	Cybersecurity IAM Analyst	-	9626165768	sreekarthikeyan0898@gmail.com	https://www.linkedin.com/in/sree-karthikeyan-a88a84187/?originalSubdomain=in
14	IBM	Arpita Majumder	Tech Consultant	-	7894369677	Arpita.majumder@ibm.com	https://www.linkedin.com/in/arpita-majumder-85612a67/
15	RnD Soft	Tamilselvan	IT Support Manager	-	9361784871	dtamilselvan1004@gmail.com	

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
2023-24	200	180	40	36	20	12
2024-25	300	180	60	40	30	12
2025-26	500	180	100	60	50	12

#The Estimated Data is an average for each state.

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
	2022-23	-	-	-	-	-	-	-	-	-

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: 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/N8231 Design processes to manage security threats and incidents across multiple technology layers	PC1. Manage access to IoT assets and systems based on identity access and management tools and frameworks	3	5	-	2
	PC2. Evaluate security threat levels and criticality of IoT assets and systems to prioritize security measures	3	5	-	2
	PC3. Define security parameters and develop encryption standards for data stored in cloud platforms and databases	3	5	-	2
	PC4. Maintain logs of data security performance metrics and analyze variances to identify issues and take action	3	5	-	2
	PC5. Conduct security assessments including penetration testing and vulnerability scans using automated and manual techniques	3	5	-	2
	PC6. Protect the IoT network and devices from unauthorized access by configuring and troubleshooting security hardware and software	3	5	-	2
	PC7. Secure the perimeter of the IoT network and classify components based on function and data sensitivity	3	5	-	2
	PC8. Employ network monitoring tools and design logging systems to detect and respond to security threats in real time	3	5	-	2
	PC9. Ensure all security policies and standards are consistently followed and security processes are managed daily	3	5	-	2
	PC10. Regularly apply security patches and employ digital certificates along with disaster recovery plans to ensure resilience	3	5	-	2
	Total Marks	**30**	**50**	**-**	**20**
SSC/N8232 Detect occurrences of security incidents to IoT solutions	PC1. record, classify and prioritize information security incidents using standard templates and tools	2	2	-	1
	PC2. access their organization's knowledge base for information on previous information security incidents and how these were managed	2	2	-	1
	PC3. participate in audit reviews	2	3	-	1
	PC4. identify the requirements of audits and prepare for audits in advance	3	4	-	2
	PC5. liaise with appropriate people to gather data/information required for audits	1	3	-	1
	PC6. provide immediate support to auditors to carry out audit tasks	1	3	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC7. carry out required audit tasks using standard tools and following established procedures/guidelines/checklists	1	3	-	1
	PC8. evaluate the impact of potential anomalies	2	2	-	1
	PC9. ensure both signature-based and anomaly-based intrusions are detected in a timely manner	2	2	-	1
	PC10. perform regular maintenance of detection processes	1	3	-	1
	PC11. ensure readiness of maintenance processes to reliable detect incidents	3	4	-	2
	PC12. apply security controls to IoT solutions in line with data security policies, procedures and guidelines	1	3	-	1
	PC13. perform security assessments of gateway / edge devices systems using automated security assessment tools	3	6	-	2
	PC14. design and develop dashboards/KPIs for monitoring the incidents, the root cause and detection to resolution corrective actions using standard Commercial off-the-shelf based Investigation Management tool	1	3	-	1
	PC15. identify critical security threats and vulnerabilities across all layers of the IoT solution	2	2	-	1
	PC16. predict and extrapolate attack trends ahead of their occurrence	2	2	-	1
	PC17. carry out backups of security devices and applications in line with security policies, procedures and guidelines	1	3	-	1
	Total Marks	**30**	**50**	**-**	**20**
SSC/N8233 Respond to detected security incidents and restore affected capabilities	PC1. plan timely response to detected security incidents	3	5	-	2
	PC2. execute post-incident processes and procedures in line with security policies, procedures, and guidelines	2	3	-	1
	PC3. automate responses to detected security threats and incidents	3	5	-	2
	PC4. assign information security incidents promptly to appropriate people for investigation/action	3	5	-	2
	PC5. track the progress of investigations into information security incidents and escalate to appropriate people where progress does not comply with standards or service level agreements (SLAs)	1	3	-	1
	PC6. liaise with stakeholders to gather, validate and provide information related to information security incidents, where required	2	2	-	1
	PC7. report to law enforcement agencies, if required	3	5	-	2
	PC8. prepare accurate preliminary reports on information security incidents using standard templates and tools	1	3	-	1
	PC9. submit preliminary reports promptly to appropriate people for action	1	3	-	1
	PC10. neutralize the effects of the security incident or mitigate it	3	4	-	2
	PC11. prevent further expansion of the security incident	1	3	-	1
	PC12. ensure timely restoration of IoT assets and systems affected by the security incident	3	5	-	2

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC13. incorporate lessons learned to prevent future security incidents	2	2	-	1
	PC14. update the organization's knowledge base promptly and accurately with information security incidents and how they were managed	2	2	-	1
	Total Marks	**30**	**50**	**-**	**20**
SSC/N8238 Create technical documents and manuals	PC1. Identify the purpose and the scope of the activity for which technical documentation is to be produced	5	11	-	3
	PC2. obtain information for the technical document from relevant sources and stakeholders	5	8	-	3
	PC3. draft technical document ensuring that content is concise, complete, and easy to consume	5	8	-	3
	PC4. review technical document content with relevant stakeholders and document owners	3	4	-	2
	PC5. ensure that technical document is formatted and designed as per specifications	3	4	-	3
	PC6. transfer technical document to relevant stakeholders for sign-off and publishing	3	4	-	3
	PC7. continuously review and update technical document	6	11	-	3
	Total Marks	**30**	**50**	**-**	**20**
SSC/N8249 Operational Technology Security	PC1. Understand OT fundamentals and the importance of security in industrial environments.	3	5	-	2
	PC2. Elaborate the difference between IT and OT environments	3	5	-	2
	PC3. Discuss OT network topology components	3	5	-	2
	PC4. Familiarize with international standards and compliance requirements.	3	5	-	2
	PC5. Learn how to implement segmentation and zone-based security and ensure OT networks are segmented from IT networks to reduce attack surface and prevent lateral movement of threats.	3	5	-	2
	PC6. Maintain an inventory of all OT devices and systems, including legacy equipment and proprietary systems not on standard networks.	3	5	-	2
	PC7. Evaluate the Common vulnerabilities in OT devices legacy hardware, firmware & conduct regular assessments tailored for industrial control systems, including firmware and hardware vulnerabilities unique to OT devices.	3	5	-	2
	PC8. Implement strict controls over modifications to OT systems to prevent accidental or malicious changes that could impact safety or operations.	3	5	-	2
	PC9. Deploy OT-optimized intrusion detection systems IDS and continuous monitoring solutions capable of handling real-time data flows and specialized protocols (e.g., Modbus, DNP3, Proprietary protocols and detect and respond to OT security incidents.	3	5	-	2
	PC10. Balance security with operational safety.	3	5	-	2
	Total Marks	**30**	**50**	**-**	**20**
	Introduction to Employability Skills	1	1	-	-
	Constitutional values – Citizenship	1	1	-	-

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
DGT/VSQ/ N0102 Employability Skills (60 Hrs)	Becoming a Professional in the 21st Century	2	4	-	-
	Basic English Skills	2	3	-	-
	Career Development & Goal Setting	1	2	-	-
	Communication Skills	2	2	-	-
	Diversity & Inclusion	1	2	-	-
	Financial and Legal Literacy	2	3		
	Essential Digital Skills	3	4		
	Entrepreneurship	2	3		
	Customer Service	1	2		
	Getting Ready for Apprenticeship & Jobs	2	3		
	Total Marks	**20**	**30**	**-**	**-**
Grand Total Marks		**170**	**280**	**-**	**100**

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.