QUALIFICATION FILE

Cybersecurity

☒ 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: 4.5

Submitted By: Namrata Kapur

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><b>1.</b></td><td><b>Qualification Name</b></td><td colspan="2"><b>Cybersecurity</b></td></tr>
<tr><td><b>2.</b></td><td><b>Sector/s</b></td><td colspan="2"><b>IT/ITeS</b></td></tr>
<tr><td><b>3.</b></td><td><b>Type of Qualification:</b> ☒ <b>New</b> ☐ <b>Revised</b> ☐ <b>Has Electives/Options</b> ☐ <b>OEM</b></td><td><b>NQR Code & version of the existing /previous qualification:</b> <i>(change to previous, once approved)</i></td><td><b>Qualification Name of the existing/previous version: Cybersecurity</b></td></tr>
<tr><td><b>4.</b></td><td><b>a. OEM Name</b>
<b>b. Qualification Name</b>
(<i>Wherever applicable</i>)</td><td colspan="2"><b>Cybersecurity</b></td></tr>
<tr><td><b>5.</b></td><td><b>National Qualification Register (NQR) Code &Version</b>
(<i>Will be issued after NSQC approval</i>)</td><td><b>QG-4.5-IT-01805-2024-V1-NASSCOM</b></td><td><b>6. NCrF/NSQF Level: 4.5</b></td></tr>
<tr><td><b>7.</b></td><td><b>Award (Certificate/Diploma/Advance Diploma/ Any Other</b>
<i>(Wherever applicable specify multiple entry/exits also & provide details in annexure)</i></td><td colspan="2">Certificate</td></tr>
<tr><td><b>8.</b></td><td><b>Brief Description of the Qualification</b></td><td colspan="2">Individuals at this job are responsible for protecting an organization’s networks, systems, and data assets. They monitor security posture through vulnerability assessment/ penetration testing and implement suitable mitigation measures and disaster recovery plans. They also possess the necessary skills to perform forensic tasks.</td></tr>
<tr><td><b>9.</b></td><td><b>Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee</b></td><td colspan="2"><b>Entry Qualification & Relevant Experience:</b>
<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 1st year of 3-year/ 4-years UG</td><td></td></tr>
<tr><td>2</td><td>Pursuing 1st year of 3-year/ 4-years UG and continuing education</td><td></td></tr>
<tr><td>3</td><td>Previous relevant Qualification of NSQF Level 4</td><td>1.5 Years of relevant experience</td></tr>
</table>
<b>Min Age: 19 Years</b></td></tr>
</table>

10.	**Credits Assigned to this Qualification, Subject to Assessment** *(as per National Credit Framework (NCrF))*	17 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)	170	340	-	-	510
Online	170	340	-	-	510

(Refer Blended Learning Annexure for details)

14.	**Aligned to NCO/ISCO Code/s** *(if no code is available mention the same)*	NCO-2015/ NIL
15.	**Progression Path After Attaining the Qualification, wherever applicable** *(Please show Professional and Academic progression)*	This entry should refer to one or more of the following: **Professional progression**: access to related qualification(s) at the next NSQF level: Chief Information Security Officer **Academic progression**: access to related qualification(s) at the next NSQF level: Software Vulnerability/ Penetration Tester, Information Security Specialist, Forensic 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**	
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: Namrata@nasscom.in** **Contact No.: 0120-4990111** **Website: https://nasscom.in**	
23.	**Final Approval Date by NSQC:06th February 2023**	**24. Validity Duration: 3 Years**	**25. Next Review Date: 06th February 2026**

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.	Work organization and management for cybersecurity	SSC/N0943 NOS Version 1	Non-Core	4.5	01	10:00	20:00	00:00	00:00	30:00	30	70	-	-	100	5%
2.	Communication and interpersonal skills for cybersecurity	SSC/N0944 NOS Version 1	Non-Core	4.5	01	10:00	20:00	00:00	00:00	30:00	30	70	-	-	100	10%
3.	Secure systems design and creation	SSC/N0945 NOS Version 1	Core	4.5	02	20:00	40:00	00:00	00:00	60:00	30	70	-	-	100	10%
4.	SSC/N0946: Secure systems operation and maintenance	SSC/N0946 NOS Version 1	Core	4.5	03	30:00	60:00	00:00	00:00	90:00	30	70	-	-	100	15%
5.	Secure Systems Protection and defense	SSC/N0947 NSQF Level 4.5	Core	4.5	06	60:00	120:00	00:00	00:00	180:00	30	70	-	-	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)*
		NOS Version 1														
6.	Operations and Management	SSC/N0948 NOS Version 1	Core	4.5	01	10:00	20:00	00:00	00:00	30:00	30	70	-	-	100	20%
7.	Intelligence collection and analysis	SSC/N0948 NOS Version 1	Core	4.5	01	10:00	20:00	00:00	00:00	30:00	30	70	-	-	100	10%
8.	Investigation and Digital Forensics	SSC/N0950 NOS Version 1	Core	4.5	02	20:00	40:00	00:00	00:00	60:00	30	70	-	-	100	15%
Duration (in Hours) / Total Marks			-	-	17	170:00	340:00	00:00	00:00	510:00	240	560	-	-	800	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)*	Graduate in Engineering/Technology/ Statistics/ Mathematics/Computer Science/Physical Sciences with Minimum 5 years of relevant experience and 2 years of full-time training experience in information and cyber security/ network engineering/ IT infrastructure
2.	**Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	Graduate in Engineering/Technology/ Statistics/ Mathematics/Computer Science/Physical Sciences with Minimum 5 years of relevant experience and 2 years of full-time training experience in information and cyber security/ network engineering/ IT infrastructure
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)*	Graduate in Engineering/Technology/ Statistics/ Mathematics/Computer Science/Physical Sciences with Minimum 5 years of relevant experience and 2 years of full-time training experience in information and cyber security/ network engineering/ IT infrastructure
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines), (wherever applicable)*	Graduate in Engineering/Technology/ Statistics/ Mathematics/Computer Science/Physical Sciences with Minimum 5 years of relevant experience and 2 years of full-time training experience in information and cyber security/ network engineering/ IT infrastructure

3.	**Lead Assessor's/Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	Graduate in Engineering/Technology/ Statistics/ Mathematics/Computer Science/Physical Sciences with a Minimum 5 years of relevant experience and 2 years of full-time training experience in information and cyber security/ network engineering/ IT infrastructure
4.	**Assessment Mode** *(Specify the assessment mode)*	Can be either in the classroom or online
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 of qualification

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): Yes
4.	Number of Industry validations provided:
5.	Estimated nos. of persons to be trained and employed:
6.	Evidence of Concurrence/Consultation with Line Ministry/State Departments: In progress 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_Cybersecurity_V1.0
9.	**Supporting Document:** Career Progression *(Mandatory-Public View)*	NA
10.	**Supporting Document:** Occupational Map *(Mandatory)*	NA
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
Professional Theoretical Knowledge/Process knowledge	• Participate in systems security implementation, configuration, and maintenance. • Monitor systems to identify security vulnerabilities, anomalies, and security breaches.	Evaluation of assets, threats, vulnerabilities, and security risks, creating a map of the security counter measures at different layers, administering the functioning of cyber security infrastructure components in various scenarios	4.5

NCrF/NSQF Level Descriptors	Key requirements of the job role/ outcome of the qualification	How the job role/ outcomes relate to the NCrF/NSQF level descriptor	NCrF/NSQF Level
	• Investigate the causes for security vulnerability/ breach. • Work effectively with colleagues and maintain a healthy and safe work environment. • Apply communication skills and interpersonal skills at workplace.	and security situations, and performing forensic analysis when needed requires the job holder to obtain specialized theoretical and practical skills, in a wide range of cybersecurity contexts.	
Professional and Technical Skills/ Expertise/ Professional Knowledge	• cyber security architecture concepts, including topology, protocols, components, and principles (e.g., application of defence-in-depth) • relevant networking concepts, devices, and terminologies • 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) • Cyber forensics concepts and tools • network traffic analysis methods and network design processes • prepare recommendations that have the potential to meet the security objectives of the organization • ensure technology risk considerations are identified and adequately addressed for new application developments, integration, and deployment	Defining security infrastructure policies, process controls and standards for an enterprise requires a thorough understanding of the business priorities, existing cybersecurity technologies, risks faced by the organization, security requirements, organizational structure, etc. To standardize security operations requires the job role holder to be factually correct and have a wide-ranging specialized theoretical skill.a	4.5
Employment Readiness & Entrepreneurship **Skills & Mind-set/Professional Skill**	• prepare recommendations that have the potential to meet the security objectives of the organization. • ensure technology risk considerations are identified and adequately addressed for new application developments, integration, and deployment	Developing remedial action plans and counter measures to maintain consistent operations of enterprise infrastructure and preparing recommendations that have the potential to meet the security objectives of the organization, require the job holder to be highly cognitive and practical in approach.	4.5

NCrF/NSQF Level Descriptors	Key requirements of the job role/ outcome of the qualification	How the job role/ outcomes relate to the NCrF/NSQF level descriptor	NCrF/NSQF Level
Broad Learning Outcomes/Core Skill	• Listen actively and communicate with others orally and in writing. • Seek input and suggestions from line managers. • Work in a dynamic environment with peers to build and maintain positive and effective customer relationships to meet their requirements. • Follow instructions, guidelines, procedures, rules, and service level agreements. • Practice active listening and verbally communicating information. • Follow quality assurance standards and produce error-free works. • Work independently and collaboratively • Use information technology to browse the internet	Individuals at this job need to have analytical skills, arithmetic and algebraic skills and communication skills to comply with and contribute to the design, automation and maintenance of security systems. The individual should be result oriented. The individual should also be able to demonstrate skills for communication, creative and logical thinking.	4.5
Responsibility	• provide the organization with considered advice on the implications of accepting, modifying, or rejecting security recommendations	Individuals in this role need to have sufficient knowledge and experience to act in an advisory capacity. They need to be able to manage small teams as well.	4.5

Annexure: Tools and Equipment (lab set-up)

Batch Size:

S. No.	Tool / Equipment Name	Specification	Quantity for specified Batch size
1	PC/Laptop with internet	With Wifi (2MBPS Dedicated)	1 Unit per Trainee
2	Relevant Software: Vulnerability assessment and penetration testing tools, SIEM tools and forensic tools	• Vulnerability Scanning tools like Qualys, Burp Suite, Tenable Nessus, Netsparker etc. • Penetration Testing tools like DirBuster, Nikto, Hydra, SQLMap, Netsparker, Burp Suite, etc. • SIEM tools like ArcSight, QRadar, RSA NetWitness Suite, Splunk, LogRythym etc.	1 Unit per Trainee

		• Operating Systems like Kali Linux, Parrot OS, Windows, MacOS etc. • Digital Forensic tools such as FTK, SleuthKit, WinHex, EnCase, X-Ways, Nuix Investigate, Redline, etc.	
3	Microphone/Voice System	For lecture & class activities	1 Unit for Trainer
4	White Board		1 Unit for Trainer
5	White Board Maker		1 Unit for Trainer
6	Projector		1 Unit

Annexure: Industry Validation Summary

S. No	Organization Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID	LinkedIn Profile *(if available)*
1							
2							
3							
4							
5							

Annexure: Training and Employment Details

Year	Total Candidates		Women		People with Disability	
	Estimated Training #	Estimated Employment Opportunities	Estimated Training #	Estimated Employment Opportunities	Estimated Training #	Estimated Employment Opportunities
2023-24	~30000	~36000	-	-	-	-
2024-25	~33000	~39000	-	-	-	-

2025-26	~46000	~42000	-	-	-	-

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

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

Annexure: Detailed Assessment Criteria

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes		Theory Marks	Practical Marks	Project Marks	Viva Marks
NOS 0943: Work organization and management for cybersecurity	PC1.	Follow health and safety standards, rules, and regulations	2	4	-	-
	PC2.	Maintain a safe working environment	2	4	-	-
	PC3.	Identify and use the appropriate Personal Protective Equipment for ESD	2	5	-	-
	PC4.	Select, use, clean, maintain, and store tools and equipment safely and securely	2	5	-	-
	PC5.	Plan the work area to maximize efficiency and maintain the discipline of regular tidying	2	5	-	-
	PC6.	Work efficiently and check progress and outcomes regularly	2	5	-	-
	PC7.	Keep up to date with ‘license to practice’ requirements and maintain currency	3	7	-	-
	PC8.	Undertake thorough and efficient research methods to support knowledge growth	3	7	-	-
	PC9.	Update and maintain security policies as needs and the field evolves	3	7	-	-
	PC10.	Plan to optimize device usage and sustainability for clients	3	7		
	PC11.	Proactively try new methods, systems, and embrace change	3	7		
	PC12.	Safety and sustainability dispose of electronic data storage devices	3	7		
	Total Marks		**30**	**70**	**-**	**-**

SSC/N0944: Communication and interpersonal skills for cyber security	PC1. Use strong listening and questioning skills to deepen understanding of complex situations	3	8	-	-
	PC2. Ensure consistently effective verbal and written communications with colleagues	3	8	-	-
	PC3. Recognize and adapt to the changing needs of colleagues	4	9	-	-
	PC4. Proactively contribute to the development of strong and effective teams	4	9	-	-
	PC5. Share knowledge and expertise with colleagues and develop supportive learning cultures	4	9	-	-
	PC6. Manage tension/anger and give individuals confidence that their problems can be resolved	4	9	-	-
	PC7. Accurately document steps taken and findings in the course of investigations	4	9	-	-
	PC8. Ensure policies and procedures for security and operation on information systems are carefully followed	4	9	-	-
	Total Marks	**30**	**70**	**-**	**-**
SSC/N0945: Secure systems design and creation	PC1. Apply cyber security and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation) when designing and documenting overall program Test & Evaluation procedures.	2	4	-	-
	PC2. Conduct independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by information technology (IT) systems to determine the overall effectiveness of controls	2	4	-	-
	PC3. Develop and conduct assessments of systems to evaluate compliance with specifications and requirements	2	4	-	-
	PC4. Secure the interoperability of systems or elements of systems incorporating IT	2	4	-	-
	PC5. Analyse the security of new or existing computer applications, software, or specialized utility programs, to provide actionable results	2	4	-	-
	PC6. Develop and maintain business, systems, and information processes, to support enterprise mission needs	2	4	-	-
	PC7. Develop information technology (IT) rules and requirements that describe baseline and target architectures	2	4	-	-

	PC8. Ensure that stakeholder security requirements necessary to protect the organization’s mission and business processes are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes	2	5	-	-
	PC9. Conduct software and systems engineering and software systems research to develop new capabilities, ensuring cyber security is fully integrated.	2	6	-	-
	PC10. Conduct research (including penetration testing) to evaluate potential vulnerabilities in cyberspace systems	2	6	-	-
	PC11. Consult with stakeholders to evaluate functional requirements and translate functional requirements into technical solutions	2	6	-	-
	PC12. Plan, prepare, and execute tests of systems	2	6	-	-
	PC13. Analyse, evaluate and report results against specifications and requirements	3	6	-	-
	PC14. Design, develop, test, and evaluate information system security throughout the systems development life cycle	3	7	-	-
	Total Marks	**30**	**70**	**-**	**-**
SSC/N0946: Secure systems operation & maintenance	PC1. Install, configure, test, operate, maintain, and manage network infrastructure	4	10	-	-
	PC2. Manage software that permits the sharing and transmission of all data	4	10	-	-
	PC3. Install, configure, troubleshoot, and maintain server configurations (hardware and software) to ensure their confidentiality, integrity, and availability	4	10	-	-
	PC4. Manage accounts in relation to access control, passwords, account creation, and administration	4	10	-	-
	PC5. Analyse organization’s computer systems and update information systems solutions to help them operate more securely, efficiently and effectively	4	10		
	PC6. Develop methods to monitor and measure risk, compliance, and assurance efforts.	5	10	-	-
	PC7. Conduct audits of information technology (IT) programs, infrastructure network to provide ongoing optimization, cyber security and problem- solving support	5	10	-	-
	Total Marks	**30**	**70**	**-**	**-**

SSC/N0947: Secure systems protection and defence	PC1. Use defensive measures and information collected from a variety of sources to identify, analyse, and report events that occur or might occur within the network to protect information, information systems, and networks from threats	3	7	-	-
	PC2. Test, implement, deploy, maintain, review, and administer the infrastructure hardware and software that are required to effectively manage the computer network and resources	3	7	-	-
	PC3. Monitor network to actively remediate unauthorized activities	3	7	-	-
	PC4. Respond to crises or urgent situations within own areas of expertise to mitigate immediate and potential threats	3	7	-	-
	PC5. Use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security Investigate and analyse all relevant response activities	3	7	-	-
	PC6. Investigate and analyse all relevant response activities	3	7		
	PC7. Conduct assessments of threats and vulnerabilities	3	7	-	-
	PC8. Determine deviations from acceptable configurations, enterprise, or local policy	3	7	-	-
	PC9. Assess the level of risk and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations	3	7	-	-
	PC10. Follow documented enterprise procedures for incident preparedness and response	3	7	-	-
	Total Marks	**30**	**70**	**-**	**-**
SSC/N0948: Operations and Management	PC1. Identify and assess the capabilities and activities of cyber security criminals or foreign intelligence entities	3	7	-	-
	PC2. Produce findings to help initialize or support law enforcement and counterintelligence investigations or activities	3	7	-	-
	PC3. Analyse collected information to identify vulnerabilities and potential for exploitation	3	8	-	-
	PC4. Analyse threat information from multiple sources, disciplines, and agencies across the Intelligence Community	3	8	-	-
	PC5. Synthesize and place intelligence information in context, draw insights about the possible implications	3	8	-	-

	PC6. Apply current knowledge of one or more regions, countries, non-state entities, and/or technologies	3	8	-	-
	PC7. Apply language, cultural, and technical expertise to support information collection, analysis, and other cyber security activities	4	8	-	-
	PC8. Identify, preserve, and use system artefacts for analysis	4	8		
	PC9. Execute successful data and systems recovery in case of loss	4	8		
	Total Marks	**30**	**70**	**-**	**-**
SSC/N0949: Intelligence collection and analysis	PC1. Execute collection using appropriate strategies and within the priorities established through the collection management process	6	14	-	-
	PC2. Perform in depth joint targeting and cybersecurity planning processes	6	14	-	-
	PC3. Gather information and develop detailed operational plans and orders supporting requirements	6	14	-	-
	PC4. Assist strategic and operational level planning across the full range of operations for integrated information and cyberspace operations	6	14	-	-
	PC5. Support activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities or to support other intelligence activities	6	14		
	Total Marks	**30**	**70**	**-**	**-**
SSC/N0950: Investigation and Digital Forensics	PC1. Trace important information through logs and other information sources to ascertain the chain of events making up the incident	5	11	-	-
	PC2. Identify the process by which an attack may have taken place to be able to evacuate the incident and the way infrastructure may be impacted	5	11		
	PC3. Deduce steps taken in an incident to identify any weaknesses existing in the systems	5	12		
	PC4. Give careful attention to detail to be able to spot and identify anomalies and patterns in data sets	5	12		
	PC5. Learn new techniques, tools and techniques as the filed evolves	5	12		
	PC6. Collect, process, preserve, analyse, and present computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations	5	12		

	Total Marks	**30**	**70**	**-**	**-**
Grand Total		**240**	**560**	**-**	**-**

Annexure: 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.

Assessment System Overview

A uniform assessment of job candidates per industry standards facilitates the industry's progress by filtering employable individuals while simultaneously providing candidates with an analysis of personal strengths and weaknesses.

Assessment Criteria

The Sector Skill Council will create criteria for assessment for each Qualification Pack. Each Performance Criteria (PC) will be assigned marks proportional to its importance in NOS. SSC will also lay down the proportion of marks for Theory and Skills Practical for each PC. The assessment for the theory part will be based on a knowledge bank of questions created by the SSC. Assessment will be conducted for all compulsory NOS and where applicable, on the selected elective/option NOS/set of NOS.

Guidelines for Assessment			
Testing Environment	**Tasks and Functions**	**Productivity**	**Teamwork**
• Carry out assessments under realistic work pressures found in the normal industry workplace (or simulated workplace). • Ensure that the range of materials, equipment, and tools that learners use are current and of the type routinely found in the normal industry workplace (or simulated workplace) environments.	• Assess that all tasks and functions are completed in a way, and to a timescale that is acceptable in the normal industry workplace. • Assign workplace (or simulated workplace) responsibilities that enable learners to meet the requirements of the NOS.	• Productivity levels must be checked to ensure that it reflects those that are found in the work situation being replicated.	• Provide situations that allow learners to interact with the range of personnel and contractors found in the normal industry workplace (or simulated workplace).

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 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 about a Qualification from the perspective of NSQF compliance. The Qualification File will be normally submitted by the awarding body for the qualification.
Sector	A grouping of professional activities based on their main economic function, product, service, or technology.

Annexure: Market Research & Gap Analysis

There is a growing requirement of cybersecurity knowledge across various industry domains and employees are willing to familiarize themselves with cybersecurity concepts.

According to a report from NASSCOM and the DSCI, India’s cybersecurity services industry is estimated to reach a total valuation of US$13.6 billion by 2025, creating thousands of job opportunities in this space. Some of the most common job roles include security specialist and penetration tester. The Hindu reported that although India had 40000 job openings for cybersecurity professionals as of May 2023, 30% of these vacancies could not be filled due to huge skill gap.

(Source: https://indbiz.gov.in/indian-cybersecurity-sector-to-hit-us13-6bn-by-2025-report/, https://www.thehindu.com/business/Industry/india-facing-huge-shortage-of-cybersecurity-professionals-teamlease/article66994515.ece)