QUALIFICATION FILE

Cyber Security Associate

☒ **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:

National Institute of Electronics and Information Technology

NIELIT Bhawan,
Plot No. 3, PSP Pocket, Sector-8,
Dwarka, New Delhi-110077,
Phone:- 91-11-2530 8300
e-mail:- contact@nielit.gov.in

Contents

Section 1: Basic Details

1.	Qualification Name	Cyber Security Associate	
2.	Sector/s	IT-ITeS	
3.	Type of Qualification: ☒ New ☐ Revised ☐ Has Electives/Options ☐OEM	NQR Code & version of existing/previous qualification: NA	Qualification Name of existing/previous version: NA
4.	a. OEM Name b. Qualification Name (*Wherever applicable*)	-	
5.	National Qualification Register (NQR) Code &Version (*Will be issued after NSQC approval*)	QG-4.5-IT-00352-2023-V1-NIELIT	6. NCrF/NSQF Level: *4.5*
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	The "Cyber Security Associate", course intends to build a sound Cyber Security professional for the industry. Carrying this belief forward the concepts of vulnerability and penetration testing and cyber forensics have been introduced so as to give a perspective to the enrolled learner about the two fields. On completing the course the enrolled candidate will possess knowledge about both fields and this will lay a solid foundation for the candidate's career progression.	
9.	Eligibility Criteria for Entry for Student/Trainee/Learner/Employee	a. Entry Qualification & Relevant Experience:	

S. No.	Academic/Skill Qualification (with Specialization - if applicable)	Required Experience (with Specialization - if applicable)
1.	- Completed 1st year of B.Tech/ BCA/ B.Sc. (CS/IT/Electronics/ allied area) **OR** - Pursuing 1st year of B.Tech/ BCA/ B.Sc. and continuous education **OR**	

	- Pursuing 3rd year of 3-year diploma (CS/IT/EC/EE/ allied branches) after 10th and continuous education **OR** - Completed 3-year diploma after 10th **OR** - Completed 2nd year of 2 year diploma in after 12th **OR** - Pursuing 2nd year of 2- year diploma after 12th and continuous education **OR** 10th Grade pass plus 2 years of vocational education(NTC) plus 1 year of NAC in IT-ITeS. **OR** - Previous relevant Qualification of Level 3 and with minimum education as 8th Grade pass and 3 years of experience in IT-ITeS Sector.

b. **Age: No Bar**

10.	**Credits Assigned to this Qualification, Subject to Assessment** *(as per National Credit Framework (NCrF))*	18 Credits	**11. Common Cost Norm Category (I/II/III)** *(wherever applicable)***:** Category II (Information and Communication Technology)
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)* ***For the candidate possessing the relevant level 4.0 certificate with relevant experience**	☒ Offline ☐ Online ☐ Blended	

☒ Offline ☐ Online ☐ Blended

Training Delivery Modes	Theory (Hours)	Practical (Hours)	OJT /Project (Hours)	ES (Hours)	Total (Hours)
Classroom (offline)	150	240	90	60	540

		The mode of delivery shall be based on the regional demand and can be offered in any of the above modes mentioned.
14.	**Aligned to NCO/ISCO Code/s** *(if no code is available mention the same)*	**NCO-2015 Code:** 2522.0201 (Security Analyst) **NCO-2015 Code:** 3513.0200 (Computer Security Specialist)
15.	**Progression path after attaining the qualification** *(Please show Professional and Academic progression)*	*Academic:* *Vertical:* *Level 5: Courses in Cyber Security: Cyber Security and Social Media Analyst* *Level 6: Courses in Cyber Security: Information Security Specialist* *Level 7: Courses in Cyber Security: Certificate Course in Ethical Hacking and Information Security* *Professional:* *Cyber Security Assistant-> Junior Cyber Security Associate-> Cyber Security Associate*
16.	**Other Indian languages in which the Qualification & Model Curriculum are being submitted**	Qualification File is available in English and Hindi.
17.	**Is similar Qualification(s) available on NQR-if yes, justification for this qualification**	☐ Yes ☒ No if yes provide URLs of similar Qualifications:

18.	**Is the Job Role Amenable to Persons with Disability**	☒ Yes ☐ No
		If "Yes", specify applicable type of Disability:
		   . *Locomotor Disability*
		  1. *Leprosy-Cured Person*
		  2. *Dwarfism*
		  3. *Muscular Dystrophy*
		  4. *Acid Attack Victims*
		
		  b. *Visual Impairment*
		    I. *Low Vision*

19.	**How Participation of Women will be Encouraged**	Participation of Women Candidates will be ensured as per Government norms. Time to time exclusive batches for women would be run for the proposed course. Funding of women batches may be generated from IT for masses scheme /other schemes launched by Govt. of India from time to time.
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 of Submitting / Awarding Body SPOC** *(In the case of CS or MS, provide details of both Lead AB & Supporting ABs)*	**Name:** Abhinav Mishra **Email:** abhinav@nielit.gov.in **Contact No.:** 8317093868 **Website:** nielit.gov.in/gorakhpur		
23.	**Final Approval Date by NSQC: 29/03/2023**	**Validity Duration: 3 years**		**Next Review Date:** *29/03/2026*

Section 2: Module Summary

NOS/s of Qualifications
1. **Fundamentals of Network and Operating System**
2. **Fundamentals of Cyber Security.**
3. **Cryptography and Ethical Hacking**
4. **Network and Infrastructure Security**
5. **Vulnerability Assessment and Penetration Testing**
6. **Cyber Forensics**
7. **Employability Skills**
8. **Project / OJT**

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	Core/ Non-Core	NCrF/ NSQF Level	Credits as per NCrF	Training Duration (Hours)			Assessment Marks			
						Th.	Pr.	Total	Th.	Pr.	Total	Weightage (%) *(if applicable)*
1	Fundamentals of Network and Operating System	NIE/ITS/N0907	Core	4.5	3	30	60	90	30	20.76	50.76	14.50
2	Fundamentals of Cyber Security.	NIE/ITS/N0908	Core	4.5	5	60	90	150	50	34.61	84.61	24.17
3	Cryptography and Ethical Hacking	NIE/ITS/N0906	Core	4.5	2	20	40	60	20	13.84	33.84	9.66
4	Network and Infrastructure Security	NIE/ITS/N0905	Core	4.5	1	10	20	30	33.33	6.92	40.25	11.5
5	Vulnerability Assessment and Penetration Testing	NIE/ITS/N0913	Core	4.5	1	15	15	30	33.33	6.92	40.25	11.5
6	Cyber Forensics	NIE/ITS/N0914	Core	4.5	1	15	15	30	33.33	6.92	40.25	11.5
					Sub-Total	150	240	390	200	90	290	82.85

S. No	NOS/Module Name	NOS/Module Code & Version	Core/ Non-Core	NCrF/ NSQF Level	Credits as per NCrF	Training Duration (Hours)			Assessment Marks			
						Th.	Pr.	Total	Th.	Pr.	Total	Weightage (%) *(if applicable)*
7	Employability Skills	DGT/VSQ/N0102	Non-Core	4.5	2	-	-	60	-	-	30	8.57
8	Project/OJT	NA	Core	4.5	3	-	-	90	-	-	30	8.57
	Duration (in Hours) /Total Marks				18	150	240	**540**	200	90	**350**	100

Assessment - Minimum Qualifying Percentage

Minimum Pass Percentage – Aggregate at qualification level: 50 % *(Every Trainee should score specified minimum aggregate passing percentage at qualification level to successfully clear the assessment.)*

Assessment Components	NOS Included	Duration* (in mins)	Marks
Theory 1: Cyber Security Associate Paper-1	NOS 1, NOS2, NOS 3	90	100
Theory 2: Cyber Security Associate Paper-2	NOS4, NOS5, NOS6	90	100
Practical Paper-1: Cyber Security Associate	NOS 1, NOS2, NOS 3 , NOS4, NOS5, NOS6	180	90
Internal Assessment/Employability Skills	NOS 7	-	30
OJT/Project	NOS 8	-	30
		Grand Total	**350**

*Assessment strategy shall be as per NIELIT Norms prevailing at times.

Section 3: Training Related

1.	**Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	O-Level (IT) / BCA / BSc (IT/CS) / Diploma in CS/IT/ allied area with 1 year of Experience in training or higher.
2.	**Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	B-LEVEL / MCA/ B.Tech in CS/IT/EC/EE/ allied areas with an experience of 2 years in training
3.	**Tools and Equipment Required for Training**	☒Yes ☐No *(If "Yes", details to be provided in Annexure)*
4.	**In Case of Revised Qualification, Details of Any Upskilling Required for Trainer**	NA

Section 4: Assessment Related

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	B-LEVEL / MCA/ B.Tech in CS/IT/EC/EE/ allied areas with an experience of 2 years in training
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	The assessor carries out theory online assessments through the remote proctoring methodology. Theory examination would be conducted online and the paper comprise of MCQ. Conduct of assessment is through trained proctors. Once the test begins, remote proctors have full access to the candidate's video feeds and computer screens. Proctors authenticate the candidate based on registration details, pre-test image captured and I- card in possession of the candidate. Proctors can chat with candidates or give warnings to candidates. Proctors can also take screenshots, terminate a specific user's test session, or re-authenticate candidates based on video feeds.
3.	**Lead Assessor's/Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	An External Examiner/ Observer (Subject matter expert) are deployed including NIELIT scientific officers who are subject expert for evaluation of Practical examination/ internal assessment / Project/ Presentation/ assignment and Major Project (if applicable). B. Tech in CS / IT / EC / EE / allied areas, MCA, B-Level 'IT' with 3 years of experience.

4.	**Assessment Mode** *(Specify the assessment mode)*	Online for Theory Online/ Offline/ Blended for other assessment components depending on the region where the assessment is conducted
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 Available in Annexure-B : Evidence of Need
2.	**Latest Market Research Reports or any other source (not older than 2 years) (Yes/No):** Yes Available in Annexure-B : Evidence of Need
3.	**Government /Industry initiatives/ requirement (Yes/No):** Yes Available in Annexure-B : Evidence of Need
4.	**Number of Industry validation provided:** 5
5.	**Estimated nos. of persons to be trained and employed:** 1000 candidates will be trained in a year.
6.	**Evidence of Concurrence/Consultation with Line Ministry/State Departments:** NIELIT is recognized as AB and AA under Government Category. NIELIT is an HRD arm of MeitY, therefore, the Line Ministry Concurrence is not required.

Section 6: Annexure & Supporting Documents Check List

Specify Annexure Name / Supporting document file name

1.	**Annexure:** NCrF/NSQF level justification based on NCrF level/NSQF descriptors *(Mandatory)*	*Available at Annexure-I: Evidence of Level*
2.	**Annexure:** List of tools and equipment relevant for qualification *(Mandatory, except in case of the online course)*	*Available at Annexure-II: Tools and Equipment*
3.	**Annexure:** Industry Validations Summary	*Available at Annexure-III: Industry Validations Summary*
4.	**Annexure:** Training & Employment Details	*Available at Annexure-IV: Training & Employment Details*

5.	**Annexure:** Blended Learning *(Mandatory, in case selected Mode of delivery is "Blended Learning")*	*Available at Annexure-V: Blended Learning*
6.	**Annexure:** Detailed Assessment Criteria	*Available at Annexure VI: Detailed Assessment Criteria*
7.	**Annexure:** Assessment Strategy	*Available at Annexure VII: Assessment Strategy*
8.	**Supporting Document:** Career Progression *(Mandatory - Public view)*	*Available at Annexure-VIII: Career Progression*
9.	**Supporting Document:** Occupational Map *(Mandatory)*	*Available at Annexure-IX: Occupational Map*
10.	**Supporting Document:** Acronym and Glossary	*Available at Annexure-X: Acronym and Glossary*
11.	**Supporting Document:** Model Curriculum *(Mandatory – Public view)*	*Available at Annexure-A: Model Curriculum*
12.	**Supporting Document:** Assessment SOP *(Mandatory)*	*Available at Annexure-C: Examination SoP*
13.	**Any other document you wish to submit:**	*NA*

Annexure I: 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	1. Gaining Knowledge of how to configure the network. 2. Gaining Knowledge of how to install and operate Linux and Windows. 3. Classification of Transmission Media and will have an in-depth idea about various networking devices. 4. Conceptualization of OSI, TCP/IP Model, and Function of layers, learn about various types of networks.	1. Possesses specialized operational knowledge and understanding of the work. 2. Have complete knowledge of the concept of time required	4.5

	5. Students will be able to conceptualize cybersecurity at different levels. 6. Students are able to define security solutions at the OS level 7. Conceptualization of Cryptography, Classical and Modern Cryptography 8. Conceptualization of Public Key Infrastructure (PKI). 9. The student will learn about the Open-source intelligence (OSINT) framework. 10. Students will understand the concept of Network Security and Network Security Protocols. 11. The Students will understand the concept of Email and their protocols, Email Spoofing and Phishing Techniques, and the concept of Fake E-mails. 12. Students are able to think critically and apply the concept of cyber security in determining best practices. 13. Students are able to think critically and apply the concept of Vulnerability Assessment 14. Students are able to think critically and apply the concept of Penetration Testing and VAPT Tools 15. The Students will understand the concept of Digital Forensics 16. The Students will understand the concept of Digital Forensics & Acquisition 17. The Students will understand the concept of File & Disk Analysis 18. The Students will understand the concept of Memory Forensics 19. The Students will understand the concept of System & Network Forensics 20. The Students will understand the concept of Logs & Reporting	for delivery; and Quality for a range of issues	
Professional and Technical Skills/ Expertise/ Professional Knowledge	1. Students will be able to Configure Network Settings and perform user and group management in Windows as well as Linux 2. Knowledge about various network administration software Utilities and network troubleshooting. 3. Knowledge about the implementation of security solutions at the OS level 4. Students will be able to use the NMAP and Wireshark tools for scanning and sniffing.	1. Possesses specialized professional and technical skills; displays clarity of professional knowledge and technical skills in a broad range of activities/ tasks. 2. Have knowledge of collecting and interpreting the available information, drawing	4.5

	5. Students will be able to manage and implement network security solutions. 6. Students will be able to Detect Network Attacks using Wireshark 7. Knowledge of Cyber Security tools and techniques. 8. Depth coverage of Cyber Security solutions ranging from their benefits to their implementation and scope and its pros and cons 9. Students are able to think critically and apply the concept of Vulnerability Assessment 10. The Students will understand the concept of Digital Forensics & Acquisition	conclusions & communicating the same	
Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	1. Introduction to Employability Skills 2. Career Development & Goal Setting 3. Becoming a Professional in the 21st Century 4. Constitutional values - Citizenship 5. Basic English Skills 6. Communication Skills 7. Essential Digital Skills 8. Financial and Legal Literacy 9. Customer Service 10. Entrepreneurship 11. Diversity & Inclusion 12. Getting Ready for Apprenticeship & Jobs	1. Can explain the Entrepreneurial Mindset and describe its importance of it in the context of opportunity curation for future jobs. 2. Can comfortably use most of the basic software with proficiency. 3. Have the ability to relate to the 5 pillars of Social Emotional Skills and describe the similarities between SES and Emotional Intelligence.	4.5
Broad Learning Outcomes/Core Skill	1. Able to troubleshoot in case of facing problems in the Operating system. 2. Conceptualize Cyber Security Concepts and would be able to understand the cyber security relates issues and challenges in Cyber World 3. Able to perform security operations on Linux and Windows OS	1. Students are able to use, create, configure the Network, and troubleshoot the network using TCP/IP command line utilities. 2. Have knowledge of the Cyber Security Project Cycle and apply Cyber Security technology to improve the security postures of the object.	4.5

Responsibility	1. Helping computer users with security products and procedures 2. Protects the system by defining access privileges, control structures, and resources. 3. Recognizes problems by identifying abnormalities; reporting violations. Implements security improvements by assessing the current situation; evaluating trends; anticipating requirements	Takes complete responsibility for delivery and quality of own	4.5

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

Batch Size: 30

S. No.	Tool / Equipment Name	Specification	Quantity for specified Batch size
1	Classroom	1 (30 Sq.m)	30
2	Student Chair	30	30
3	Student Table	30	30
4	Desktop computer with accessories	16 GB RAM, Camera, Headset with Microphone CentOS/Ubuntu Linux Kali Linux Windows 10,, VirtualBox, Open-Source Antivirus Open Source or Native Firewall Software	30
5	Desk jet printer	1 Nos.	01

Classroom Aids

The aids required to conduct sessions in the classroom are:

1. LCD Projector

2. WhiteBoard

Annexure III: Industry Validations Summary

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

S. No	Organization Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID
1	Essential InfoSec Private Limited	Mr.Pawan Srivastava	Director	Essential InfoSec Private Limited, Mehrauli-Gurgaon Road Near Sultanpur Metro Station, Sultanpur, Delhi 110030	7985534793	pawan@essentialinfosec.com
2	Accretive Technologies Private Limited	Mr. Manish Nanda	Managing Director	World Tech Tower, Plot No. C-203, Phase 8-B, Mohali 160 055 Punjab	9814302885	manish@accretivetechno.com
3	OST Electronics Pvt Ltd.	Amarjit Singh	Manager - Tech Support	SCO 212, Sector 36-D, Sector 36, Chandigarh, 160036	9815936460	amarjit.singh@ostindia..com
4	Fore Solution (P) ltd	Manu Mehta	Director	Fore Solution (P) ltd SCO: 365-66, First Floor, Sector 35, Chandigarh, 160022	9814010307	manu@foresolution.net
5	Spectra Computech Pvt. Ltd.	N.P Singh	Manager Marketing	4th Floor, Godrej Eternia Building Plot No. 70, Industrial Area Phase I, Chandigarh, 160002	9876023966	npsingh@spectracomputech.com
6	Buannel Studio Pvt. Ltd	Lalrimguala	CEO	Aizwal, Mizoram	8732856261	pslalringual@gmail.com
7	United Computer	Subhasis Choudhury	Chief Executive	Chotonilpur (Pirtala), P.O. Sripally, Burdwan-713103	9641820965	united-computer97@rediffmail.com

Annexure IV: Training & Employment Details

Training and Employment Projections:

Year	Total Candidates		Women		People with Disability	
	Estimated Training #	Estimated Employment Opportunities	Estimated Training #	Estimated Employment Opportunities	Estimated Training #	Estimated Employment Opportunities
2023	1000	100	200	100	10	2
2024	1000	100	200	100	10	2
2025	1000	100	200	100	10	2

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

Annexure V: Blended Learning

Blended Learning Estimated Ratio & Recommended Tools:

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	Online interaction platforms like JitSi Meet, Bharat VC, Google Meet, MS Teams, etc.	60:40
2	Imparting Soft Skills, Life Skills, and Employability Skills /Mentorship to Learners	Online interaction platforms like JitSi Meet, Bharat VC, Google Meet, MS Teams, etc.	60:40
3	Showing Practical Demonstrations to the learners	Online interaction platforms like JitSi Meet, Webex, Bharat VC, Google Meet, MS Teams, etc.	60:40

4	Imparting Practical Hands-on Skills/ Lab Work/ workshop/ shop floor training	NA	100:0
5	Tutorials/ Assignments/ Drill/ Practice	Online interaction platforms like JitSi Meet, Bharat VC, Google Meet, MS Teams, etc.	50:50
6	Proctored Monitoring/ Assessment/ Evaluation/ Examinations	NIELIT Remote Proctored Software	Online: 100% Theory Offline: 100% Practical
7	On the Job Training (OJT)/ Project Work Internship/ Apprenticeship Training	Simulated Platform	Either 100% online on virtual environment Or 100% offline in the Industry.

Annexure VI: 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
NOS 1: Fundamentals of Network and Operating System	1. Overview of OSI, TCP/IP Model, and Function of layers, learn about various types of networks. 2. Knowledge about the Benefits of Networks, components of Computer Networks and also have an insight into various topologies used in networking. 3. Explain various Transmission modes, Ethernet, and the Classification of Transmission Media. 4. In-depth idea about various networking devices like Repeaters, Hubs, Bridges, Switches, and routers 5. Introduction to TCP/IP Protocol Model in Depth, Port Numbers, Common TCP& UDP Ports and also Some important TCP/IP protocols. 6. IP addressing, Classes, IP Addressing Scheme, Subnetting Basics along with How to Create Subnets, Subnet Masks, Subnetting Class C Addresses, Subnetting Class B Addresses and VLSM.	30	20.76

	7. Configure ip addresses in Windows and Linux and also have a proper introduction to RIR, registries and IANA along with attaining knowledge about TCP/IP Troubleshooting utilities, Troubleshooting IP Addressing 8. The in-depth idea about the Windows operating system and its File System 9. The in-depth idea about the Linux operating system and its File System 10. Working on Command Line Utilities, 11. Managing Users and Groups, 12. Configuring Permissions, Read, Write, and Execute: 13. Preparing the File System for ACLs 14. Configuring Administrator Tasks with sudo 15. Working with Links: Working with Symbolic Links, Working with Hard Links		
NOS 2: Fundamentals of Cyber Security	1. Gaining the basic idea of Information Security 2. Introduction to Ethical Hacking 3. Overview of Cryptography 4. Exploring OS security 5. Using Security Tools for Windows Operating System 6. Gaining the idea of Wireless Networks and Wireless Security 7. Gaining the idea of the Android and iPhone iOS Operating system 8. Introduction to Web Application & its terminologies 9. Exploring Web Application Protocols 10. Configuring Browser Security 11. Introduction to Social Media & its security 12. Exploring Security in Digital Payment Systems 13. Gaining the idea of Various kinds of fraud in banking and Cyber Crime 14. Introduction to Cyber Law, Cyber Cell, and Cyber Fraud Helpline	50	34.61

NOS 3: Cryptography and Ethical Hacking	1. Overview of Cryptography 2. Gaining an idea of Public Key Infrastructure (PKI) 3. Exploring Scanning and Information Gathering 4. Exploring Open-source intelligence (OSINT) framework 5. Gaining the idea to use the NMAP and Wireshark tools for scanning and sniffing. 6. Gaining the idea of Detecting Network Attacks using Wireshark. 7. Gaining the idea of MITM Attacks and their Countermeasures. 8. Gaining an idea on the types of password attacks. 9. Understand the Hash function, Hash algorithm, Password Hashes, and Password Cracking Countermeasures. 10. Gaining the idea of the various types of Spoofing. 11. Gaining an idea of Denial of Service and Countermeasures 12. Gaining an idea of Steganography 13. Gaining an idea of E-Mail Security	20	13.84
NOS 4: Network and Infrastructure Security	1. Understand the concept of Network Security and Network Security Protocols. 2. Understand the Attacks at Layer 3 and Layer 2 of OSI model 3. Gaining the idea of the CAM Table and CAM Flooding Attacks. 4. Gaining the idea and Configuring the Switch Port Security and Switch Port Violations. 5. Preventing CAM Flooding Attacks by using Switch Port Security. 6. Understand the concept of Network Security Controls and Network Access controls. 7. Understand the concept of Firewalls, DMZ, VPN, IDS, IPS, and Network Traffic Monitoring and Analysis. 8. Gaining the idea of IP Security, Protocols used in IPSec, the Security Architecture of IPSec, and Modes of IPSec. 9. Understand the concept of Intrusion Detection. 10. Understand the concept of SOC, NOC, and the Functions of SOC. 11. Gaining the idea of SIEM and Security Operations and Management	33.33	6.92

NOS 5: Vulnerability Assessment and Penetration Testing	1. Understand the concept of Vulnerability Assessment and its Goals & Objectives 2. Understand the concept of OWASP Framework. 3. Comparision of OWASP Top 10(2017) and OWASP Top 10 (2021). 4. Understand the concept of OWASP's Top 10 vulnerabilities. 5. Understand the concept of Broken Access Control, Cryptographic Failures, and Injection. 6. Understand the concept of Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components. 7. Understand the concept of Identification and Authentication Failures. 8. Understand the concept of Software and Data Integrity Failures. 9. Understand the concept of Security Logging and Monitoring Failures. 10. Understand the concept of Server Side Request Forgery (SSRF). 11. Understand the concept of Penetration Testing and Penetration testing methodology, Types of penetration. 12. Understand the working of the Metasploit Framework.	33.33	6.92
NOS 6: **Cyber Forensics**	1. Understand the concept of Digital Forensics and the Objectives of Digital Forensics. 2. Understand the concept of the Elements of a Digital Crime and the Process of Digital Forensics. 3. Understand the concept of Digital Evidence. 4. Understand the concept of Methodology for Digital Investigators. 5. Understand the concept of Evidence Collection Methods. 6. Understand the concept of Disk Imaging and Disk Cloning. 7. Understand the types of Data Acquisition, Storage Formats and Acquisition Methods,\. 8. Understand the concept of Data Representation and Files Examination. 9. Understand the concept ofd File Structure and File Analysis. 10. Understand the process of Investigating Deleted Files, Formatted Disks, File Carving and File System Analysis. 11. Understand the concept of Network Forensics. 12. Understand the concept of Logging Infrastructure. 13. Using Linux Tools for Log Analysis, Web Logs, Windows Events, and Syslog.	33.33	6.92

NOS 7: Employability Skills	Explanation of the following: 1. Need for employability skills 2. Various constitutional and personal values. 3. Different environmentally sustainable practices and their importance 4. 21st-century skills and their importance 5. How to use the basic spoken English language 6. Do's and don'ts of effective communication 7. Inclusivity and its importance 8. Different types of disabilities and appropriate communication and behavior towards PwD 9. Different types of financial products and services 10. How to compute income and expenses 11. Importance of maintaining safety and security in financial transactions 12. Different legal rights and laws 13. How to operate digital devices and applications safely and securely 14. Ways to identify business opportunities 15. Types of customers and their needs 16. How to apply for a job and prepare for an interview 17. Apprenticeship scheme and the process of registering on the apprenticeship portal	30
NOS 8: OJT/Project	NOS 8: OJT/Project Demonstration of Cyber Security Project	30
	Grand Total	350

Annexure VII: Assessment Strategy

Assessment of the qualification evaluates candidates to ascertain that they can integrate knowledge, skills and values for carrying out relevant tasks as per the defined learning outcomes and assessment criteria.

The underlying principle of assessment is fairness and transparency. The evidence of the outcomes and assessment criteria. competence acquired by the candidate can be obtained by conducting Theory (Online), Practical assessment, Internal assessment, Project/Presentation/ Assignment, Major Project. The emphasis is on the practical demonstration of skills & knowledge gained by the candidate through the training. Each OUTCOME is assessed & marked separately. A candidate is required to pass all OUTCOMES individually based on the passing criteria.

About Examination Pattern:

1. The question papers for the theory and practical exams are set by the Examination wing (assessor) of NIELIT HQS.

2. The assessor assigns roll number.

3. The assessor carries out theory online assessments through remote proctoring methodology. Theory examination would be conducted online and the paper comprise of MCQ. Conduct of assessment are through trained proctors. Once the test begins, remote proctors have full access to candidate's video feeds and computer screens. Proctors authenticate the candidate based on registration details, pre-test image captured and I- card in possession of the candidate. Proctors can chat with candidates or give warnings to candidates. Proctors can also take screenshots, terminate a specific user's test session, or re-authenticate candidates based on video feeds.

4. An External Examiner/ Observer may be deployed including NIELIT officials for evaluation of Practical examination/ internal assessment / Project/ Presentation/. Major Project (if applicable) would be evaluated preferably by external/ subject expert including NIELIT officials.

5. Pass percentage would be 50% marks in each component.

6. Candidates may apply for re-examination within the validity of registration (only in the assessment component in which the candidate failed).

7. For re-examination prescribed examination fee is required to be paid by the candidate only for the assessment component in which the candidate wants to reappear.

8. There would be no exemption for any paper/module for candidates having similar qualifications or skills.

9. The examination will be conducted in English language only.

Quality assurance activities: A pool of questions is created by a subject matter expert and moderated by other SME. Test rules are set beforehand. Random set of questions which are according to syllabus appears which may differ from candidate to candidate. Confidentiality and impartiality are maintained during all the examination and evaluation processes.

Annexure-VIII: Career Progression

Academic:

Vertical:

Level 5: Courses in Cyber Security: Cyber Security and Social Media Analyst

Level 6: Courses in Cyber Security: Information Security Specialist

Level 7: Courses in Cyber Security: Certificate Course in Ethical Hacking and Information Security

Professional:

Cyber Security Assistant-> Junior Cyber Security Associate-> Cyber Security Associate

Annexure IX: Acronym and Glossary

Acronym

Acronym	Description
AA	Assessment Agency
AB	Awarding Body
ISCO	International Standard Classification of Occupations
NCO	National Classification of Occupations
NCrF	National Credit Framework
NOS	National Occupational Standard(s)
NQR	National Qualification Register
NSQF	National Skills Qualifications Framework
OJT	On-the-Job Training

Glossary

Term	Description
National Occupational Standards (NOS)	NOS define the measurable performance outcomes required from an individual engaged in a particular task. They list down what an individual performing that task should know and also do.
Qualification	A formal outcome of an assessment and validation process which is obtained when a competent body determines that an individual has achieved learning outcomes to given standards
Qualification File	A Qualification File is a template designed to capture necessary information of a Qualification from the perspective of NSQF compliance. The Qualification File will be normally submitted by the awarding body for the qualification.
Sector	A grouping of professional activities on the basis of their main economic function, product, service or technology.
Long Term Training	Long-term skilling means any vocational training program undertaken for a year and above. https://ncvet.gov.in/sites/default/files/NCVET.pdf