QUALIFICATION FILE–Standalone NOS

Cyber Security for Cloud Infrastructure

☐ Horizontal/Generic ☐Vertical/Specialization

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

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

NCrF/NSQF Level: 5

Submitted By:

National Institute of Electronics and Information Technology (NIELIT)

NIELIT Bhawan,
Plot No. 3, PSP Pocket, Sector-8,
Dwarka, New Delhi-110077,
Phone: - 91-11-25308300
e-mail: - contact@nielit.gov.in

Table of Contents

Section 1: Basic Details

1.	**NOS-Qualification Name**	**Cyber Security for Cloud Infrastructure**	
2.	**Sector/s**	**IT-ITeS**	
3.	**Type of Qualification** ☒ **New** ☐ **Revised**	**NQR Code & version of the existing /previous qualification:**	**Qualification Name of the existing/previous version:**
4.	**National Qualification Register (NQR) Code & Version**	NG-05-IT-01428-2023-V1-NIELIT	**5. NCrF/NSQF Level:** 5
6.	**Brief Description of the Standalone NOS**	The "Cybersecurity for Cloud Infrastructure" upskilling course is designed to equip participants with the essential knowledge and skills needed to secure cloud-based environments. Participants delve into the intricacies of cloud security, learning to identify and mitigate potential threats and vulnerabilities specific to cloud infrastructure. The course covers key cybersecurity principles, such as access control, encryption, and network security, tailored to the dynamic landscape of cloud computing. Through hands-on exercises and real-world case studies, participants gain practical experience in implementing security measures to safeguard data and applications in the cloud. This course is invaluable for cybersecurity professionals, cloud architects, and IT professionals looking to enhance their expertise in ensuring the robust security of cloud infrastructure. The curriculum emphasizes a holistic approach to cybersecurity, addressing challenges unique to cloud environments. Participants explore security best practices for popular cloud platforms, develop skills in threat detection and incident response, and gain an understanding of compliance and regulatory considerations in cloud security. By the end of the program, participants are well-prepared to navigate the complexities of securing cloud infrastructure, contributing to resilient and protected cloud-based systems in various organizational settings.	

<table>
<tr><td><b>7.</b></td><td><b>Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee</b></td><td colspan="2"><b>a. Entry Qualification &Relevant Experience:</b>
<table>
<tr><th>S. No.</th><th>Academic/Skill Qualification (with Specialization - if applicable)</th><th>Relevant Experience (with Specialization - if applicable)</th></tr>
<tr><td>1</td><td>Pursuing^ Final Year B.Tech in any branch of Engineering*
Or
Pursuing^ Final Year MCA
Or
Pursuing^ Final Year B.Sc. in any branch of Sciences*
Or
Pursuing^ Final Year B.Sc. in IT/CS/Electronics/allied subjects
*Students should have relevant knowledge of the Networking and programming concepts.
#Students with the above entry requirements are eligible to take the course subject to clearing the written test comprising of Analytical Reasoning, Mathematics and English
^Passout students in the above entry requirements are also eligible for the course.</td><td>NA</td></tr>
</table>
<b>b. Age:</b> 21 Years</td></tr>
<tr><td><b>8.</b></td><td><b>Credits Assigned to this NOS-Qualification, Subject to Assessment</b> <i>(as per National Credit Framework (NCrF))</i></td><td>4</td><td><b>9. Common Cost Norm Category (I/II/III)</b> <i>(wherever applicable)</i>: Category-II</td></tr>
<tr><td><b>10.</b></td><td><b>Any Licensing Requirements for Undertaking Training on This Qualification</b> <i>(wherever applicable)</i></td><td colspan="2">Not Applicable</td></tr>
</table>

<table>
<tr><td><b>11.</b></td><td><b>Training Duration by Modes of Training Delivery</b><i>(Specify <b>Total Duration</b> as per selected training delivery modes and as per requirement of the qualification)</i></td><td>☒ <b>Offline</b> ☐ <b>Online</b> ☐ <b>Blended</b>
<table>
<tr><th>Training Delivery Mode</th><th>Theory (Hours)</th><th>Practical (Hours)</th><th>Total (Hours)</th></tr>
<tr><td><b>Classroom (offline)</b></td><td>60</td><td>60</td><td>120</td></tr>
</table>
The mode of delivery shall be based on the regional demand and can be offered in any of the above modes mentioned.</td></tr>
<tr><td><b>12.</b></td><td><b>Assessment Criteria</b></td><td>
<table>
<tr><th>Theory (Marks)</th><th>Practical (Marks)</th><th>Project (Marks)</th><th>Viva (Marks)</th><th>Total (Marks)</th><th>Passing %age</th></tr>
<tr><td>100</td><td>0</td><td>0</td><td>0</td><td>100</td><td>50</td></tr>
</table>
The centralised online assessment is conducted by the Examination Wing, NIELIT Headquarters.</td></tr>
<tr><td><b>13.</b></td><td><b>Is the NOS Amenable to Persons with Disability</b></td><td>☒ <b>Yes</b> ☐ <b>No</b>
<b>If “Yes”, specify applicable type of Disability:</b>
<b>a.</b> Locomotor Disability: Leprosy Cured Person, Dwarfism, Muscular Dystrophy and Acid Attack Victims
<b>b.</b> Visual Impairment: Low Vision</td></tr>
<tr><td><b>14.</b></td><td><b>Progression Path After Attaining the Qualification, wherever applicable</b></td><td>Cloud Security Architect
Cloud Security Analyst
Cloud Security Consultant
Cloud Penetration Tester
Incident Responder(Cloud)</td></tr>
<tr><td><b>15.</b></td><td><b>How will the participation of women be encouraged?</b></td><td>Participation by women can be ensured through Government Schemes. Occasionally, exclusive batches for women would be run for the proposed courses. Funding is available for women’s participation under other schemes launched by the Government from time to time.</td></tr>
<tr><td><b>16.</b></td><td><b>Other Indian languages in which the Qualification & Model Curriculum are being submitted</b></td><td>Qualification files available in English & Hindi Language.</td></tr>
<tr><td><b>17.</b></td><td><b>Is similar NOS available on NQR-if yes, justification for this qualification</b></td><td>☐<b>Yes</b> ☒ <b>No</b></td></tr>
</table>

18.	**Name and Contact Details Submitting / Awarding Body SPOC** *(In the case of CS or MS, provide details of both Lead AB & Supporting ABs)*	A. Name: SHRI NILADRI DAS Position in the organization: Scientist E Address: NIELIT Agartala Tel number(s): 8794028299 E-mail address: niladridas@nielit.gov.in B. Name: SHRI BINOY DAS Position in the organization: Senior Technical Officer Address: NIELIT Agartala Tel number(s): 8794822459 E-mail address: erbinoy@nielit.gov.in	
19.	**Final Approval Date by NSQC: 30/11/2023**	**20. Validity Duration: 3 years**	**21. Next Review Date: 30/11/2026**

Section 2: Training Related

1.	**Trainer's Qualification and experience in the relevant sector (in years) (as per NCVET guidelines)**	B.Tech or Equivalent as per NCrF with 15+ years of experience
2.	**Master Trainer's Qualification and experience in the relevant sector (in years) (as per NCVET guidelines)**	B.Tech or Equivalent as per NCrF with 15+ years of experience
3.	**Tools and Equipment Required for the Training**	☒ Yes ☐No Available at Annexure-II
4.	**In Case of Revised NOS, details of Any Upskilling Required for Trainer**	Not Applicable

Section 3: Assessment Related

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	B.Tech or Equivalent as per NCrF with 15+ years of experience
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines), (wherever applicable)*	The assessor carries out theory online assessments through the remote proctoring methodology. Theory examination would be conducted online and the paper comprises 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)*	External Examiners/ Observers (Subject matter experts) are deployed including NIELIT scientific officers who are subject experts for evaluation of Practical examination/ internal assessment / Project/ Presentation/ assignment and Major Project (if applicable). Qualification is generally B.Tech.
4.	**Assessment Mode***(Specify the assessment mode)*	Centralized online examination will be conducted
5.	**Tools and Equipment Required for Assessment**	Same as for training ☒ Yes ☐ No

Section 4: Evidence of the Need for the Standalone NOS

1.	Government /Industry initiatives/ requirement (Yes/No): Yes.
2.	Number of Industry validation provided: 4
3.	Estimated number of people to be trained: 1000 persons per year shall be trained.
4.	Evidence of Concurrence/Consultation with Line/State Departments (In case of regulated sectors): No NIELIT is recognised as AB and AA under the Government Category. NIELIT is the HRD arm of MeitY, GoI.

Section 5: Annexure & Supporting Documents Check List

Specify Annexure Name / Supporting document file name

1.	**Annexure:** NCrF/NSQF level justification based on NCrF/NSQF descriptors *(Mandatory)*	*Available at* Annexure-I: Evidence of Level
2.	**Annexure:** List of tools and equipment relevant for NOS *(Mandatory, except in case of online course)*	*Available at* Annexure-II: Tools and Equipment
3.	**Annexure: Industry Validation**	*Available at* Annexure-III: Industry Validation
4.	**Annexure: Training Details**	*Available at* Annexure-IV: Training Details
5.	**Annexure:** Blended Learning *(Mandatory, in case the selected Mode of delivery is Blended Learning)*	*Available at* Annexure-V: Blended Learning
6.	**Annexure/Supporting Document:** Standalone NOS- Performance Criteria Details Annexure/Document with PC-wise detailing as per NOS format (Mandatory- Public view)	*Available at* Annexure-VI: Performance Criteria
7.	**Annexure:** Performance and Assessment Criteria *(Mandatory)*	*Available at* Annexure-VII: Detailed Assessment Criteria
8.	**Annexure:** Assessment Strategy *(Mandatory)*	*Available at* Annexure-VIII: Assessment Strategy
9.	**Annexure:** Acronym and Glossary *(Optional)*	*Available at* Annexure-IX: Acronym and Glossary
10.	**Supporting Document:** Model Curriculum	*Available at* Annexure-A: Model Curriculum

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	This course necessitates a robust theoretical foundation in various key areas. Professionals must acquire in-depth knowledge of cloud computing architectures, and understand the nuances of cloud security models and technologies. Theoretical expertise in access control mechanisms, encryption protocols, and network security principles specific to cloud environments is essential. Additionally, a comprehensive understanding of cybersecurity frameworks, threat landscapes, and compliance standards relevant to cloud infrastructure is crucial. This theoretical knowledge equips professionals to design, implement, and manage robust cybersecurity measures tailored to the complexities of cloud-based systems, ensuring the protection and integrity of data and applications	This course is aligned with higher NSQF/NCrF levels, indicating a need for advanced theoretical knowledge and practical application in the specialized field of Cybersecurity and Cloud Security.	5
Professional and Technical Skills/ Expertise/ Professional Knowledge	Professionals must acquire in-depth knowledge of cloud computing architectures, understanding the nuances of cloud security models and technologies. Theoretical expertise in access control mechanisms, encryption protocols, and network security principles specific to cloud environments is essential. Additionally, a comprehensive understanding of cybersecurity frameworks, threat landscapes, and compliance standards relevant to cloud infrastructure is crucial. This theoretical knowledge equips professionals to design, implement, and manage robust cybersecurity measures tailored to the complexities of cloud-based systems, ensuring the protection and integrity of data and applications.	Individuals completing this qualification are likely to possess the expertise required for roles demanding advanced and specialized knowledge in the field of cloud security.	5

Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	This course enhances employment readiness by providing individuals with sought-after technical skills in cloud security, threat detection, and incident response. Additionally, the program cultivates entrepreneurship skills by instilling a strategic understanding of cybersecurity frameworks, enabling professionals to contribute to innovative solutions and entrepreneurial ventures in the dynamic field of cloud security.	Candidates will be learning effective communications which will make them smart in communicating with various companies and people.	5
Broad Learning Outcomes/Core Skill	The "Cybersecurity for Cloud Infrastructure" course delivers broad learning outcomes by equipping participants with comprehensive knowledge and skills to secure cloud environments. Learners gain expertise in implementing cybersecurity measures specific to cloud infrastructure, covering access control, encryption, threat detection, and incident response for ensuring the resilience and protection of cloud-based systems.	Candidate can perform well under supervision of team lead	5
Responsibility	This course is responsible for preparing professionals to effectively identify, assess, and mitigate cybersecurity risks in cloud environments. It ensures that participants can apply robust security measures, adhere to best practices, and contribute to the development of secure cloud infrastructures within their respective organizations.	Takes complete responsibility for delivery and quality of own work and output as also the subordinates. Shares responsibility for the group tasks.	5

Annexure II: Tools and Equipment (lab set-up)

List of Tools and Equipment
Batch Size: 30

S. No.	Tool / Equipment Name	Specification	Quantity for specified Batch size
1	Classroom	1 (30 Sq.m)	30
2	Students Chair	30	30
3	Students Table	30	30

4	Desktop computer with accessories	GUI based Operating System, CentOS/Ubuntu Linux, Kali Linux Windows 10, VirtualBox, Open-Source Antivirus, Open Source or Native Firewall Software	30
5	Deskjet printer	1 No.	Paper-A4

Classroom Aids for offline and blended mode of training:

The aids required to conduct sessions in the classroom are:

1. LCD Projector/Smart Board
2. Pin-up Board
3. WhiteBoard, Markers

Annexure III: Industry Validations/ Government Recognition Summary

S. No	Organization Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID
1	Software World	Amrita Saha	Proprietor	Ujan Abhoynagar, Manipuripara, Agartala, Tripura(West)	7005261744	support@softwareworld.Co.In
2	Bada Biplab Power Solution LLP	Iduli Debbarma	Designated Partner	Agartala West Tripura, Pin: 799003	9436740983	bbpsllp@gmail.com
3	Krishna Industrial Services	Debajit Dey	Proprietor	Badharghat Chowmuhani Agartala, Pin: 799003	9862770077	jbyacademy@gmail.com
4	JB Youth Computer Solution & Educational Society	Nishi Kanta Das	Project Coordinator	Badharghat Chowmuhani, Siddi Ashram, Agartala	9436740983	jbyacademy@gmail.com

Annexure IV : Training Details

Training Projections:

Year	Estimated Training # of Total Candidates	Estimated training# of Women	Estimated training# of People with Disability
2023-24	1000	200	20
2024-25	1000	200	20
2025-26	1000	200	20

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

Annexure V: Blended Learning

Blended Learning Estimated Ratio &Recommended Tools:

Refer NCVET "Guidelines for Blended Learning for Vocational Education, Training & Skilling" available on:

S. No.	Select the Components of the NOS	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	NA	NA
3	Showing Practical Demonstrations to the learners	Online interaction platforms like JitSi Meet, Bharat VC, Google Meet, MS Teams, etc.	60:40
4	Imparting Practical Hands-on Skills/ Lab Work/ workshop/ shop floor training	PCs/Laptops	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 Online Examination	Online: 100% Theory
7	On the Job Training (OJT)/ Project Work Internship/ Candidate Training	NA	NA

Annexure VI : Standalone NOS- Performance Criteria details

1. Description:

This upskilling course is designed to empower participants with the knowledge and skills needed to secure cloud-based systems effectively. Covering key cybersecurity principles such as access control, encryption, and threat detection specific to cloud environments, participants learn to navigate the unique challenges posed by cloud infrastructure. Through a combination of theoretical insights and practical exercises, this course equips cybersecurity professionals and IT experts with the expertise to implement robust security measures and ensure the resilience of cloud-based systems against evolving cyber threats.

2. Scope:

The scope covers the following:

- Aligns with industry demands, offering participants a skill set crucial for roles in cloud security, a field experiencing rising significance.
- Equipped to pursue specialized positions as cloud security specialists, addressing the specific challenges of securing cloud-based systems effectively.
- Skills acquired in this course are applicable and valuable in a wide range of industries, emphasizing its broad and enduring relevance.

3. Elements and Performance Criteria

Elements	Performance Criteria
Advanced Concepts on Cyber Security	PC1: Demonstrate a comprehensive understanding of fundamental cybersecurity terminology, accurately using key terms in discussions and written communication. PC2: Apply foundational principles from the "Foundations of Networking" module to design, configure, and troubleshoot basic network setups, showcasing the ability to implement secure networking practices. PC3: Execute security measures within operating systems, demonstrating the application of OS Security principles to safeguard systems from potential vulnerabilities and unauthorized access. PC4: Assess and implement web security measures, showcasing the ability to identify and mitigate potential threats and vulnerabilities in web-based applications and services. PC5: Demonstrate the ability to effectively respond to cybersecurity incidents by applying incident

	response management principles, including timely identification, containment, eradication, recovery, and lessons learned.
Cloud Security	PC1: Demonstrate a detailed understanding of cloud computing concepts, encompassing key components such as service models, deployment models, and the benefits and challenges associated with cloud environments. PC2: Assess and compare the features, offerings, and service-level agreements of different cloud service providers, demonstrating the ability to make informed decisions based on specific organizational requirements and considerations. PC3: Execute fundamental security practices in the cloud, including identity and access management, encryption, and network security, showcasing proficiency in establishing a secure foundation for cloud-based operations. PC4: Implement and evaluate security measures specific to cloud infrastructure, including securing virtual machines, containers, and network configurations, showcasing the ability to safeguard cloud resources effectively. PC5: Integrate compliance and governance principles into cloud environments, demonstrating the ability to align cloud practices with regulatory requirements, industry standards, and organizational policies to ensure a secure and compliant cloud infrastructure.

4. Knowledge and Understanding (KU):

The individual on the job needs to know and understand:

KU1. Imparts foundational Knowledge and Understanding (KU) by delving into the principles and practices of securing cloud-based systems.

KU2. Participants gain insights into the unique cybersecurity challenges posed by cloud infrastructure, understanding the nuances of protecting data, applications, and network resources in cloud environments.

KU3. Covers access control mechanisms, encryption protocols, and network security strategies tailored specifically to the dynamic nature of cloud computing.

KU4. Learners acquire knowledge of threat detection and incident response methodologies, developing the skills needed to identify and mitigate cybersecurity risks in real-time.

KU5. Emerge with a well-rounded understanding of cybersecurity best practices, enabling them to contribute effectively to the security posture of cloud infrastructures within their professional roles.

5. Generic Skills (GS):

User/individual on the job needs to know how to:

GS1. Follow instructions, guidelines and procedures

GS2. Listen effectively and communicate information accurately

GS3. Apply formatting features to achieve the desired results

Annexure VII: Assessment Criteria

Detailed PC-wise assessment criteria and assessment marks for the NOS are as follows:

S. No.	Assessment Criteria for Performance Criteria	Theory Marks	Practical Marks	Project Marks	Viva Marks
Advanced Concepts on Cyber Security	PC1: Demonstrate a comprehensive understanding of fundamental cybersecurity terminology, accurately using key terms in discussions and written communication. PC2: Apply foundational principles from the "Foundations of Networking" module to design, configure, and troubleshoot basic network setups, showcasing the ability to implement secure networking practices. PC3: Execute security measures within operating systems, demonstrating the application of OS Security principles to safeguard systems from potential vulnerabilities and unauthorized access. PC4: Assess and implement web security measures, showcasing the ability to identify and mitigate potential threats and vulnerabilities in web-based applications and services. PC5: Demonstrate the ability to effectively respond to cybersecurity incidents by applying incident response management principles, including timely identification, containment, eradication, recovery, and lessons learned.	50	-	-	-

Cloud Security	PC1: Demonstrate a detailed understanding of cloud computing concepts, encompassing key components such as service models, deployment models, and the benefits and challenges associated with cloud environments. PC2: Assess and compare the features, offerings, and service-level agreements of different cloud service providers, demonstrating the ability to make informed decisions based on specific organizational requirements and considerations. PC3: Execute fundamental security practices in the cloud, including identity and access management, encryption, and network security, showcasing proficiency in establishing a secure foundation for cloud-based operations. PC4: Implement and evaluate security measures specific to cloud infrastructure, including securing virtual machines, containers, and network configurations, showcasing the ability to safeguard cloud resources effectively. PC5: Integrate compliance and governance principles into cloud environments, demonstrating the ability to align cloud practices with regulatory requirements, industry standards, and organizational policies to ensure a secure and compliant cloud infrastructure.	50	-	-	-
Total Marks		**100**	**-**	**-**	**-**

Annexure VIII: 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 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) examination.

About Examination Pattern:

1. The question papers for the theory 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. Theory examination would be conducted online and the paper comprise of MCQ
4. Pass percentage would be 50% marks.
5. 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 IX : 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

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.