QUALIFICATION FILE – Standalone NOS

Cloud Cybersecurity -Google

☐ Horizontal/Generic ☒ Vertical/Specialization

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

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

NCrF/NSQF Level: 5.5

Submitted By:

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

Table of Contents

Section 1: Basic Details

<table>
<tr><td>1.</td><td>NOS-Qualification Name</td><td colspan="2">Cloud Cybersecurity –Google</td></tr>
<tr><td>2.</td><td>Sector/s</td><td colspan="2">IT-ITeS SSC Nasscom</td></tr>
<tr><td>3.</td><td>Type of Qualification ☒ New ☐ Revised</td><td>NQR Code & version of the existing /previous qualification: (change to previous, once approved)</td><td>Qualification Name of the existing/previous version: (previous, once approved)</td></tr>
<tr><td>4.</td><td>National Qualification Register (NQR) Code & Version (Will be issued after NSQC approval.)</td><td>NG-5.5-IT-02983-2024-V1-NASSCOM</td><td>5. NCrF/NSQF Level: 5.5</td></tr>
<tr><td>6.</td><td>Brief Description of the Standalone NOS</td><td colspan="2">This learning path consists of a curated collection of on-demand courses that provide authentic, interactive experience using Google Cloud technologies essential to roles in cybersecurity. Cloud security analysts are uniquely positioned as the first line of defense in protecting organizational cloud assets from a wide array of cyber-related crimes. To aid in the fight against these costly and invasive attacks on digital data and cloud infrastructure, cloud security analysts frequently focus their attention on identifying threats, risks, and vulnerabilities. Then, they respond to and defend against a variety of security incidents that can harm organizations.</td></tr>
<tr><td>7.</td><td>Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee</td><td colspan="2">a. Entry Qualification & Relevant Experience:
<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></td><td>-3rd year of 3 year or 4 year UG program(stem)
- Pursuing 3rd year of 3 year or 4 year UG program(stem)</td><td>Prerequisites:
+ Basic proficiency in foundational cloud and cybersecurity concepts, skills, and tools.
+ Basic proficiency with network security, threat analysis, Security Information and Event Management (SIEM) technologies, Linux and SQL,</td></tr>
</table></td></tr>
</table>

		<table><tr><td></td><td></td><td>and incident detection and documentation</td></tr></table> **b. Age:** 18 years old or older
8.	**Credits Assigned to this NOS-Qualification, Subject to Assessment** *(as per National Credit Framework (NCrF))*	3 **9. Common Cost Norm Category (I/II/III)** *(wherever applicable)***:**
10.	**Any Licensing Requirements for Undertaking Training on This Qualification** *(wherever applicable)*	No
11.	**Training Duration by Modes of Training Delivery** *(Specify **Total Duration** as per selected training delivery modes and as per requirement of the qualification)*	<table><tr><th>Training Delivery Mode</th><th>Theory (Hours)</th><th>Practical (Hours)</th><th>Total (Hours)</th></tr><tr><td>**Classroom (offline)**</td><td></td><td></td><td></td></tr><tr><td>**Online**</td><td>70</td><td>20</td><td>90</td></tr></table> ☐ **Offline Only** ☒ **Online Only** ☐ **Blended** *(Refer Blended Learning Annexure for details)*
12.	**Assessment Criteria**	<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>64</td><td>36</td><td></td><td></td><td>100</td><td>100</td></tr></table> *Online remotely invigilated assessment conducted by IT-ITeS SSC

13.	**Is the NOS Amenable to Persons with Disability**	**☒ Yes ☐ No** **If "Yes", specify applicable type of Disability:** *Visual Impairment (ie. Blindness), Physical Disability, and Disability caused due to chronic neurological conditions*	
14.	**Progression Path After Attaining the Qualification, wherever applicable** *(Please show Professional and Academic progression)*	Cloud Security Analyst -> Cloud Security Engineer -> Senior Cloud Security Engineer/Architect -> Cloud Security Manager	
15.	**How participation of women will be encouraged?**	Our vision at Google Cloud is to create products that work for all and to have the most inclusive experience(s) for developers. We will continue to push our vision forward by encouraging the launch of our courses at universities with a strong women's presence.	
16.	**Other Indian languages in which the Qualification & Model Curriculum are being submitted**	*(Please provide assurance and plan for developing the qualification in other Indian Languages as per training requirement)* **N/A**	
17.	**Is similar NOS available on NQR-if yes, justification for this qualification**	**☐ Yes ☒ No URLs of similar Qualifications:**	
18.	**Name and Contact Details Submitting / Awarding Body SPOC** *(In case of CS or MS, provide details of both Lead AB & Supporting ABs)*	**Name: Ericka Brown (Malone)** **Email: erickabrown@google.com** **Name: Sana Noor** **Email: sanoor@google.com** **Name: Namrata Kapur (nasscom)** **Email: Namrata@nasscom.in** **Website: Link to Course**	
19.	**Final Approval Date by NSQC: 27th August 2024**	**20. Validity Duration: 3 Years**	**21. Next Review Date: 27th August 2027**

Section 2: Training Related

1.	**Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	**Post-Graduate or Professor in IT with a minimum of 4 years experience in Cloud Engineering or its equivalent**
2.	**Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	**Post-Graduate or Professor in IT with a minimum of 4 years experience in Cloud Engineering or its equivalent**
3.	**Tools and Equipment Required for the Training**	☒Yes ☐No *(If "Yes", details to be provided in Annexure) Computer and/or Laptop with an updated browser, preferably Google Chrome. Connected to the Internet with strong bandwidth/signal.*
4.	**In Case of Revised NOS, details of Any Upskilling Required for Trainer**	If the course changes drastically, Google Cloud will communicate course changes.

Section 3: Assessment Related

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	**Post-Graduate or Professor in IT with a minimum of 4 years experience in Cloud Engineering or its equivalent**
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines), (wherever applicable)*	**N/A**
3.	**Lead Assessor's/Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	**Post-Graduate or Professor in IT with a minimum of 4 years experience in Cloud Engineering or its equivalent**
4.	**Assessment Mode** *(Specify the assessment mode)*	**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 4: Evidence of the Need for the Standalone NOS

Provide Annexure/Supporting documents name.

1.	Government /Industry initiatives/ requirement (Yes/No): Industry Initiative
2.	Number of Industry validation provided: N/A
3.	Estimated number of people to be trained: **We do not track this information.**
4.	Evidence of Concurrence/Consultation with Line/State Departments (In case of regulated sectors): (Yes/No):N/A If "No", why:

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)*	*Complete*
2.	**Annexure:** List of tools and equipment relevant for NOS *(Mandatory, except in case of online course)*	*N/A*
3.	**Annexure:** Performance and Assessment Criteria *(Mandatory)*	*Complete*
4.	**Annexure:** Assessment Strategy *(Mandatory)*	*Complete*
5.	**Annexure:** Blended Learning *(Mandatory, in case selected Mode of delivery is Blended Learning)*	*N/A*
6.	**Annexure:** Acronym and Glossary *(Optional)*	*N/A*
7.	**Annexure/Supporting Document:** Standalone NOS-Performance Criteria Details Annexure/Document with	*Complete*

	PC-wise detailing as per NOS format (Mandatory- Public view)	
8.	**Supporting Document:** Model Curriculum *(Mandatory – Public view)*	*Complete*

Annexure: Evidence of Level

NCrF/NSQF Level Descriptors	Key requirements of the job role/ outcome of the qualification	How the job role/ outcomes relate to the NCrF/NSQF level descriptor	NCrF/NSQF Level
Professional Theoretical Knowledge/Process	• Define cybersecurity as it applies to cloud computing. • Explain the security lifecycle and key concepts in cloud security computing. • Describe the fundamentals of digital transformation within the cloud. • Explain and analyze the risk management process and its main components and objects. • Explain the process and frameworks of cloud security risk management. • Define security controls and describe the control-to-risk mapping process. • Explore the stages of the compliance lifecycle and discuss the roles of control mapping, auditing, regulatory compliance, and organizational impacts of non-compliance. • Identify risk management regulations and industry standards. • Compare and contrast the regulations and industry standards that different industries adopt. • Describe the rationale for compliance and how people, process, and technology all play a part. • Describe identity and access management concepts in the cloud.	• Advanced knowledge about a multi-disciplinary/ interdisciplinary/ cross disciplinary field of technology/ skills/ job role, with specialized in depth knowledge in one or more related fields.	5.5

	• Identify elements of AAA (authentication, authorization, and auditing) for enhanced cloud security. • Explore the importance of credential handling and certificate management in cloud security. • Explain capabilities and best practices that streamline asset and resource management. • Identify common security vulnerabilities and assess their impact and risk. • Define key implementations of cloud-native concepts, including containers, serverless functions, and orchestrators. • Analyze effective practices for securing containers and Kubernetes. • Describe the role of data protection and privacy in organizational security. • Evaluate the significance of automation in cloud infrastructure. • Identify emerging trends and technologies and their impact on threat and vulnerability management. • Identify logging systems in a cloud environment and how to aggregate, correlate, and identify security alerts. • Explain how security monitoring systems are implemented and configured in a cloud computing environment. • Define incident response and how this applies to a cloud computing environment.		

	• Define the lifecycle of a security incident and the process to identify, document, and prevent future incidents. • Explain the purpose of a Disaster Recovery Plan and how this affects data retention and recovery.		
Professional and Technical Skills/ Expertise/ Professional Knowledge	• Analyze how Security Command Center and Risk Manager, as well as multi-cloud cloud security posture management, monitor compliance and help manage risk. • Implement tools for compliance risk mitigation. • Compose custom queries using pattern matching techniques and system specific syntax against aggregated logs, limiting the scope to security related information. • Configure security monitoring systems to identify and mitigate threats to a cloud environment. • Refer to attack mitigation techniques using custom defined rules, security applications, and analysis of emerging threats.	• Skills to adapt to the future of work and to the demands of the fast pace of innovations and technological developments. • Possesses a range of advanced cognitive, professional and technical skills required for performing and accomplishing complex tasks relating to the chosen fields of technology/ skills/ job role. • Wide range of cognitive and practical skills required to create innovative and feasible solutions to complex problems and situations in uncertain environment.	5.5
Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	• Describe the common roles and responsibilities of an entry-level cloud security analyst. • Identify common tools used by entry-level cloud security analysts. • Explain IAM and the scope of permissions and roles, and the roles and responsibilities of a security organization. • Identify the regulatory requirements and standards that apply to different industries.	• Organizing, analyzing, interpreting and acting on the information and effectively communicating and presenting/ using its outcome for decision making. • A keen sense of observation, enquiry, and capability for asking relevant/ appropriate questions,	5.5

	• Practice resume and interview techniques for a cloud security career.		
Broad Learning Outcomes/Core Skill	• Interpret and identify risks and vulnerabilities. • Develop a plan to protect an organization by detecting, responding, and recovering from security threats and incidents.	• Applies advance theoretical knowledge and specialized professional and technical skills involving complex variable environment and contexts • Effective understanding, monitoring and supervision of critical parameters and KPIs or others, • Evaluation and improvement of processes, procedures and work or study activities	5.5
Responsibility	• Effectively communicate security risks and recommendations to stakeholders	• At level 5.5 the candidate is a Manager/ Technical Manager/ product Manager or equivalent. • Is responsible for managing a bigger independent unit/ business activity/ project • The exercise of full personal responsibility and accountability for the initiatives undertaken and the outputs/outcomes of own work as well as of the group as a team member/ leader	5.5

Annexure: Tools and Equipment (lab set-up)

List of Tools and Equipment

Batch Size:

S. No.	Tool / Equipment Name	Specification	Quantity for specified Batch size

Classroom Aids

The aids required to conduct sessions in the classroom are:

1.
2.

Annexure: Industry Validations Summary

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

Annexure: Training Details

Training Projections: We do not track this information.

Year	Estimated Training # of Total Candidates	Estimated training # of Women	Estimated training # of People with Disability

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

Annexure: Blended Learning

Blended Learning Estimated Ratio & Recommended Tools:

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

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

Annexure: Standalone NOS- Performance Criteria details

1. Description:

This program prepares learners for entry-level roles in cloud cybersecurity. A college degree is not a prerequisite, but learners should have familiarity with foundational cloud and cybersecurity concepts, skills, and tools. These can include the basics of network security, threat analysis, Security Information and Event Management (SIEM) technologies, Linux and SQL, and incident detection and documentation. Supplemental content on these concepts is included within the course for learners who do not have this prior knowledge.

2. Scope:

The scope covers the following:

- There are five courses in Google Cloud Cybersecurity. In each course, learners will complete hands-on labs that allow them to practice key skills and produce work examples to show potential employers. The first four courses progressively build learners' working knowledge of networks, security models, and tools used to assess and address threats, risks, and vulnerabilities. The final course includes a capstone project that focuses on applying learning principles from courses 1 -4 and prepares learners to establish a career in the cloud security field.
- Contains: 5 courses | 19 modules | 212 videos | 12 labs | 154 readings | 94 quizzes | 1 capstone

3. Elements and Performance Criteria

Mandatory Modules

Course 1 - Introduction to Security Principles in Cloud Computing - 15 hours

To be competent, the user/individual on the job must be able to:
PC1. Explain how this program will help prepare learners for a career in cloud security.
PC2. Define cybersecurity as it applies to cloud computing.
PC3. Describe the common roles and responsibilities of an entry-level cloud security analyst.
PC4. Identify common tools used by entry-level cloud security analysts.

PC5. Explain the security lifecycle and key concepts in cloud security computing.

PC6. Describe the fundamentals of digital transformation within the cloud.

Course 2 - Strategies for Cloud Security Risk Management - 20 hours

To be competent, the user/individual on the job must be able to:
PC7. Analyze the key components and objects of the risk management process.
PC8. Explore cloud security risk frameworks.
PC9. Define and map security controls.
PC10. Identify the regulatory requirements and standards that apply to different industries.
PC11. Explore stages of the compliance lifecycle, emphasizing control mapping, auditing, regulatory compliance, and organizational impacts of non-compliance.

PC12. Analyze how Google Security Command Center, Risk Manager, and multi-cloud security posture management tools monitor compliance and aid in risk management.

Course 3 - Cloud Security Risks: Identify and Protect Against Threats - 25 hours

To be competent, the user/individual on the job must be able to:
PC13. Describe fundamental identity and access management concepts specific to the cloud.
PC14. Identify key components of AAA (authentication, authorization, auditing) for strengthened cloud security.
PC15. Explain capabilities and best practices for efficient asset and resource management in the cloud.
PC16. Identify common security vulnerabilities and evaluate their impact and risk mitigation strategies.
PC17. Define essential implementations of cloud-native concepts, encompassing containers, serverless functions, and orchestrators.

Course 4 - Detect, Respond, and Recover from Cloud Cybersecurity Attacks - 22 hours

To be competent, the user/individual on the job must be able to:
PC18. Analyze logging systems in a cloud environment.
PC19. Compose custom queries using pattern matching techniques.
PC20. Configure security monitoring systems to efficiently identify and mitigate threats to a cloud environment.
PC21. Define the lifecycle of a security incident and the process to identify, document, and mitigate future incidents.
PC22. Explain the purpose of a disaster recovery plan and how it affects data retention and recovery.

Course 5 - Put It All Together: Prepare for a Cloud Security Analyst Job - 8 hours

To be competent, the user/individual on the job must be able to:
PC23. Identify and assess vulnerabilities related to a security incident in a cloud environment.
PC24. Apply cloud security best practices related to backup and recovery, firewall, and identity and access management (IAM) to remediate vulnerabilities and misconfigurations.
PC25. Identify and resolve compliance issues to maintain organizational compliance with regulatory requirements.
PC26. Create a final report that provides a comprehensive review of a security incident.
PC27. Develop career resources for a role in cloud security computing.

PC28. Prepare and practice interview techniques for a cloud security career.

4. Knowledge and Understanding (KU):

The individual on the job needs to know and understand:

KU1. Describe how cybersecurity functions within a cloud environment
KU2. Problem solve using security concepts
KU3. Think analytically about security fundamentals
KU4. Interpret and compare different frameworks
KU5. Investigate threat detection reports and security compliance reports
KU6. Identify capabilities and best practices that streamline asset and resource management
KU7. Assess common vulnerabilities' risk and impact
KU8. Use tools to check for vulnerabilities
KU9. Identify data protection mechanisms and privacy laws and regulations
KU10. Monitor cloud infrastructure for potential security incidents
KU11. Participate in a cloud incident response process
KU12. Develop a security protection plan
KU13. Analyze and respond to a data breach
KU14. Create work examples to share with prospective employers
KU15. Showcase cloud security skills, knowledge, and technical expertise during interviews

5. Generic Skills (GS):

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

GS1. Understand basic principles of a Google Cloud Security Analyst.
GS2. Collaborate with a team in a Google Cloud environment.

Annexure: Assessment Criteria

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

PC No.	Assessment Criteria for Performance Criteria	Theory Marks	Practical Marks	Project Marks	Viva Marks
	Course: Introduction to Security Principles in Cloud Computing	**13**	**2**		
PC1.	Explain how this program will help prepare learners for a career in cloud security.	**1**			
PC2.	Define cybersecurity as it applies to cloud computing.	**2**			
PC3.	Describe the common roles and responsibilities of an entry-level cloud security analyst.	**2**			
PC4.	Identify common tools used by entry-level cloud security analysts.	**2**			
PC5.	Explain the security lifecycle and key concepts in cloud security computing.	**3**	**2**		
PC6.	Describe the fundamentals of digital transformation within the cloud.	**3**			
	Course: Cloud Security Risks: Identify and Protect Against Threats	**19**	**2**		
PC7.	Analyze the key components and objects of the risk management process.	**2**			
PC8.	Explore cloud security risk frameworks.	**3**			
PC9.	Define and map security controls.	**3**			
PC10.	Identify the regulatory requirements and standards that apply to different industries.	**3**			
PC11.	Explore stages of the compliance lifecycle, emphasizing control mapping, auditing, regulatory compliance, and organizational impacts of non-compliance.	**4**			
PC12.	Analyze how Google Security Command Center, Risk Manager, and multi-cloud security posture management tools monitor compliance and aid in risk management.	**4**	**2**		
	Course: Strategies for Cloud Security Risk Management	**10**	**10**		
PC13.	Describe fundamental identity and access management concepts specific to the cloud.	**2**	**2**		

PC14.	Identify key components of AAA (authentication, authorization, auditing) for strengthened cloud security.	**2**	**2**		
PC15.	Explain capabilities and best practices for efficient asset and resource management in the cloud.	**2**	**2**		
PC16.	Identify common security vulnerabilities and evaluate their impact and risk mitigation strategies.	**2**	**2**		
PC17.	Define essential implementations of cloud-native concepts, encompassing containers, serverless functions, and orchestrators.	**2**	**2**		
	Course: Detect, Respond, and Recover from Cloud Cybersecurity Attacks	**10**	**10**		
PC18.	Analyze logging systems in a cloud environment.	**2**	**2**		
PC19.	Compose custom queries using pattern matching techniques.	**2**	**2**		
PC20.	Configure security monitoring systems to efficiently identify and mitigate threats to a cloud environment.	**2**	**2**		
PC21.	Define the lifecycle of a security incident and the process to identify, document, and mitigate future incidents.	**2**	**2**		
PC22.	Explain the purpose of a disaster recovery plan and how it affects data retention and recovery.	**2**	**2**		
	Course: Put It All Together: Prepare for a Cloud Security Analyst Job	**12**	**12**		
PC23.	Identify and assess vulnerabilities related to a security incident in a cloud environment.	**2**	**2**		
PC24.	Apply cloud security best practices related to backup and recovery, firewall, and identity and access management (IAM) to remediate vulnerabilities and misconfigurations.	**2**	**2**		
PC25.	Identify and resolve compliance issues to maintain organizational compliance with regulatory requirements.	**2**	**2**		
PC26.	Create a final report that provides a comprehensive review of a security incident.	**4**	**4**		
PC27.	Develop career resources for a role in cloud security computing.	**1**	**1**		
PC28.	Prepare and practice interview techniques for a cloud security career.	**1**	**1**		
Grand Total		**64**	**36**		

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.

This section includes the processes involved in identifying, gathering, and interpreting information to evaluate the learner on the required competencies of the program.

Assessment Process Overview: Criteria for assessment for each Standalone NOS will be created by the IT-ITeS Sector Skill Council. Each Performance Criteria (PC) will be assigned marks proportional to its importance in NOS. IT-ITeS SSC will also lay down the proportion of marks for Theory and Skills Practical for each PC.

The assessment for the qualification will be based on a knowledge bank of questions created by the IT-ITeS SSC which may be requested from the OEM in the form of a Question Bank. Basis the questions that have been realized for assessment; a Blueprint shall be created. Once the Blueprint is created, the Mock assessment and actual assessment is developed in the form of multiple sets of questions to maintain the antagonistic nature of assessment.

Testing Environment: Assessment will be conducted online via an approved assessment agency and will be remotely invigilated. This entire process is managed by the Assessment Agency in conjunction with the guidelines from NCVET.

Assessment Quality Assurance: IT-ITeS SSC is responsible for the development and periodic review of the question bank developed for a specific Standalone NOS.

Assessment Documentation: The learners taking the assessment of the Standalone NOS upon training completion will be offered Credits, which can be accumulated in the Academic Bank of Credits. IT-ITeS SSC stores the digital repository of the result sheets for all assessments and issues a Digital Certificate with the detailed scores to the learner.

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

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.