QUALIFICATION FILE

IT Forensic Analyst

☒ Short Term Training (STT) ☐ Long Term Training (LTT) ☐ Apprenticeship
☒ Upskilling ☐ Dual/Flexi Qualification ☐ For ToT
☐ For ToA

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

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

1.	**Qualification Name**	**IT Forensic Analyst**	
2.	**Sector/s**	**IT/IteS**	
3.	**Type of Qualification: ☐ New ☒ Revised ☐ Has Electives/Options ☐ OEM**	**NQR Code & version of the existing /previous qualification:** *QG-06-IT-01560-2023-V1.1-NASSCOM and version 3*	**Qualification Name of the existing/previous version: IT Forensic Specialist**
4.	**a. OEM Name** **b. Qualification Name** *(Wherever applicable)*	***IT Forensic Analyst***	
5.	**National Qualification Register (NQR) Code &Version** (*Will be issued after NSQC approval*)	***QG-5.5-IT-045882025-V2-NASSCOM and version 4***	**6. NCrF/NSQF Level: 5.5**
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**	An IT Forensic analyst is responsible for a comprehensive range of tasks aimed at investigating digital incidents and preserving evidence. This includes ensuring necessary authorizations are in place for conducting forensic evidence seizure and securing physical scenes to prevent unauthorized access and protect evidence from alteration or damage. They identify potential sources of data, handle digital devices carefully, and utilize forensic tools to collect both volatile and non-volatile data, ensuring data integrity and proper documentation of chain of custody. The specialist conducts thorough examinations of extracted data, including network traffic, call data records, and emails, while analyzing metadata and digital logs to detect unauthorized access and identify anomalous activities. They participate in incident response activities, develop data recovery methods, and collaborate with law enforcement agencies when necessary. Accurate documentation of investigative activities, including logs and reports summarizing findings and methodologies, is crucial. Additionally, they conduct risk assessments, stay updated on relevant laws and regulations, and implement quality control measures. Continuous learning through workshops and conferences	

<table>
<tr><td></td><td></td><td colspan="2">helps the specialist remain informed on new technologies and methodologies in the field, while establishing ethical guidelines ensures privacy considerations are upheld during investigations.</td></tr>
<tr><td>9.</td><td>Eligibility Criteria for Entry for a Student/Trainee/Learner/Employee</td><td colspan="2">a. Entry Qualification & Relevant Experience:

*Relevant Experience in job roles related to IT/Computer Science/Cybersecurity/IT Forensics
The relevant experience would include work, internship and apprenticeship after completing relevant educational qualifications.
** PG or UG or diploma with courses related to Engg./ Science

<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 3rd year UG**</td><td>-</td></tr>
<tr><td>2</td><td>Completed 3-Year Diploma after 10th</td><td>3 years of relevant experience*</td></tr>
<tr><td>3</td><td>Previous Relevant qualification of NSQF level 5</td><td>1.5 years of relevant experience*</td></tr>
</table>

b. Age: NA</td></tr>
<tr><td>10.</td><td>Credits Assigned to this Qualification, Subject to Assessment (as per National Credit Framework (NCrF))</td><td>18 Credits</td><td>11. Common Cost Norm Category (I/II/III) (wherever applicable): II</td></tr>
<tr><td>12.</td><td>Any Licensing Requirements for Undertaking Training on This Qualification (wherever applicable)</td><td colspan="2">NA</td></tr>
</table>

<table>
<tr><td>13.</td><td>Training Duration by Modes of Training Delivery (Specify Total Duration as per selected training delivery modes and as per requirement of the qualification)</td><td>☐ Offline Only ☐ Online Only ☒ Blended
<table><tr><th>Training Delivery Mode</th><th>Theory (Hours)</th><th>Practical (Hours)</th><th>OJT (Mandatory) Hours</th><th>OJT (Recommended) Hours</th><th>Total (Hours)</th></tr><tr><td>Classroom (offline)</td><td>160</td><td>290</td><td>90</td><td></td><td>540</td></tr><tr><td>Online</td><td>160</td><td>290</td><td>90</td><td></td><td>540</td></tr></table>(Refer Blended Learning Annexure for details)</td></tr>
<tr><td>14.</td><td>Aligned to NCO/ISCO Code/s (if no code is available mention the same)</td><td>NCO-2015/ NIL</td></tr>
<tr><td>15.</td><td>Progression Path After Attaining the Qualification, wherever applicable
(Please show Professional and Academic progression)</td><td>This entry should refer to one or more of the following:
Professional progression: Access to related qualification(s) at the next NSQF level – Sr. IT Forensic Specialist, Chief Information Officer, Chief Information Security Officer, etc.
Academic progression: Access to other qualifications at the same NSQF level – Senior Consultant-Network Security, Architect Application Security, Security Infrastructure Specialist, Security Operations Centre Specialist, etc.</td></tr>
<tr><td>16.</td><td>Other Indian languages in which the Qualification & Model Curriculum are being submitted</td><td>Hindi</td></tr>
<tr><td>17.</td><td>Is similar Qualification(s) available on NQR-if yes, justification for this qualification</td><td>☐ Yes ☒ No URLs of similar Qualifications:</td></tr>
<tr><td>18.</td><td>Is the Job Amenable to Persons with Disability</td><td>☐ Yes ☒ No
If “Yes”, specify applicable type of Disability:</td></tr>
<tr><td>19.</td><td>How participation of women will be encouraged?</td><td>The Program is gender neutral although to increase the women participation, organizations are keeping aside few seats to encourage the female candidates</td></tr>
<tr><td>20.</td><td>Are Greening/Environment Sustainability Aspects covered (Specify the NOS/Module which Covers it)</td><td>☒ Yes ☐ No, DGT/VSQ/N0102: Employability Skills (60 Hours)</td></tr>
<tr><td>21.</td><td>Is Qualification suitable to be offered in Schools/Colleges</td><td>Schools: ☐ Yes ☒ No Colleges ☒ Yes ☐ No</td></tr>
</table>

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 Kapoor** **Email: Standards@nasscom.in** **Contact No.: 0120-4990111** **Website: https://www.sscnasscom.com/**	
23.	**Final Approval Date by NSQC: 07th October 2025**	**24. Validity Duration: 3 Years**	**25. Next Review Date: 7th October 2028**

Section 2: Module Summary

NOS/s of Qualifications

(In exceptional cases these could be described as components)

Mandatory NOS/s:

Specify the training duration and assessment criteria at NOS/Module level. For Further details refer curriculum document.

Th.-Theory **Pr.**-Practical **OJT**-On the Job 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.	Identify, preserve, and seize digital/electronics devices or records for investigation of possible breach or crime	SSC/N0929, V3.0	Core	5.5	05	41:00	79:00	30:00	00:00	150:00	30	50	-	20	100	21
2.	Extract relevant data or information from digital forensic evidence	SSC/N0930, V3.0	Core	5.5	05	45:00	75:00	30:00	00:00	150:00	30	50	-	20	100	21

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)
3.	Analyze information or data extracted from digital forensic evidence	SSC/N0931, V3.0	Core	5.5	05	45:00	90:00	15:00	00:00	150:00	30	50	-	20	100	21
4.	Report & present the results of a forensic investigation	SSC/N0932, V3.0	Core	5.5	01	05:00	10:00	15:00	00:00	30:00	30	50	-	20	100	21
5.	Employability Skills (60 Hours)	DGT/VSQ/N0102, V1.0	Non-Core	4	02	24:00	36:00	00:00	00:00	60:00	20	30	-	-	50	16
Duration (in Hours)/Total Marks					**18**	**160:00**	**290:00**	**90:00**	**00:00**	**540:00**	**140**	**230**	**-**	**80**	**450**	**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.																

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)*
2.																
Duration (in Hours) / Total Marks																

Assessment - Minimum Qualifying Percentage

Assessment - Minimum Qualifying Percentage
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.)

Section 3: Training Related

1.	**Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	**Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science) **Industry & training experience:** 2 years of industry experience in Cybersecurity. The industry experience would include work, internship, and apprenticeship undertaken after regular graduation **Certification:** "Trainer" mapped to the Qualification Pack "MEP/Q2601" Minimum accepted score is 80% aggregate
2.	**Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	**Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science) **Industry & training experience:** 4 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **Certification:** "Master Trainer" mapped to the Qualification Pack "MEP/Q2602" Minimum accepted score is 90% aggregate
3.	**Tools and Equipment Required for the Training**	☒Yes ☐No *(If "Yes", details to be provided in Annexure)*

4.	**In Case of Revised Qualification, details of Any Upskilling Required for Trainer**	NA

Section 4: Assessment Related

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	**Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science) **Industry & Training Experience:** 2 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **Certification:** "Assessor" mapped to the Qualification Pack "MEP/Q2701" Minimum accepted score is 80% aggregate.
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines), (wherever applicable)*	**Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science) **Industry & Training Experience:** 2 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **Certification:** "Assessor" mapped to the Qualification Pack "MEP/Q2701" Minimum accepted score is 80% aggregate.
3.	**Lead Assessor's/Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	**Educational Qualification:** Graduate (Engineering/ Technology/ Computer Science) **Industry & Training Experience:** 4 years of industry experience in Cybersecurity. The full-time experience would include work, internship, and apprenticeship undertaken after regular graduation. **Certification:** "Lead Assessor" mapped to the Qualification Pack "MEP/Q2702" Minimum accepted score is 90% aggregate.
4.	**Assessment Mode** *(Specify the assessment mode)*	The assessment will consist of a blend of hands-on practical evaluations, viva-voce, and online proctored scenario-based multiple-choice questions ensuring a thorough evaluation of the individual's proficiency in learning outcomes, practical understanding, and real-world application of concepts.
5.	**Tools and Equipment Required for Assessment**	☒ Same as for training ☐ Yes ☐ No *(details to be provided in Annexure-if it is different for Assessment)*

Section 5: Evidence of the Need for the Qualification

Provide Annexure/Supporting documents name.

1.	Latest Skill Gap study (not older than 2 years) (Yes/No): 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): Industry Initiatives
4.	Number of industry validations provided: 21
5.	Estimated number of people to be trained and employed: NA
6.	Evidence of Concurrence/Consultation with Line/State Departments: 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)*	Acronym and Glossary
7.	**Annexure:** Acronym and Glossary *(Optional)*	Acronym and Glossary
8.	**Supporting Document:** Model Curriculum *(Mandatory-Public View)*	MC_SSCQ0922_IT Forensic Analyst_V4
9.	**Supporting Document:** Career Progression *(Mandatory-Public View)*	Occupational Map-Cybersecurity

10.	**Supporting Document:** Occupational Map *(Mandatory)*	Occupational Map-Cybersecurity
11.	**Supporting Document:** Assessment SOP *(Mandatory)*	NA
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	**Identify, preserve, and seize digital/electronic devices or records for investigation of possible breach or crime** • ensure that the scene is secured to prevent unauthorized access and alteration or damage of the evidence as per containment policies and situational considerations • survey area and identify potential sources of data that could be evidence • identify and obtain materials related to digital communications which are relevant to the investigation • create a plan that prioritizes the sources, establishing the order in which the computing devices or records can be acquired • use forensic tools to collect volatile data	Forensics is a highly specialised field, and the role of a specialist in the field has to be an expert in the domain. Their work entails huge legal and financial implications for an organisation. A forensic specialist is responsible for the complete area of identifying, preserving, and seizing digital/electronic forensic evidences, extracting information and data from the digital information or data sources or devices, examining and analysing the information or data and further reporting and presenting the findings before competent authority, which involve a combination of variable routine and nonroutine tasks in unpredictable circumstances, given the nature of the job role.	5.5

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
	• duplicate non-volatile data sources to collect their data, securing the original non-volatile data sources • verify and preserve the integrity of the data source device or record in accordance with investigation procedures • carefully document each stage of the seizure and investigation • ensure chain of custody is followed for all digital media acquired in accordance with the rules of evidence **Extract relevant data or information from digital forensic evidences** • create an image or copy of the original storage device using clean storage media to have a backup • identify data that is required to be extracted and most likely sources • select the best method and tools for extraction as per the make and model of device • locate the required files and electronic data manually or using forensic tools • hunt for files and information that have been hidden, deleted, or lost		

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
	• identify presence of encrypted data or the use of steganography and the feasibility of decryption or extracting embedded data • identify the encryption method by examining the file header, identifying encryption programs installed on the system, or finding encryption keys • extract the embedded data by finding the stego key, or by using brute force and cryptographic attacks to determine a password • crack, disable, or bypass passwords placed on individual files, as well as OS passwords using various utilities and techniques • find, recover, and copy data from disks that may have been hidden, encrypted or damaged, etc. • obtain relevant information from ISP and cloud service provider after taking due authorisation from Law Enforcement Authority/Agency **Analyse information or data extracted from digital forensic evidences** • perform analysis of the extracted data using various forensic tools		

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
	• perform data hiding analysis for detecting and recovering data and may indicate knowledge, ownership, or intent • analyse programs and files in various ways to provide insight into the capability of the system and the knowledge of the user • analyse file metadata typically through the application that created it to provide insight into detailed information like authorship, time last edited, number of times edited, and print or saved location, etc. • determine ownership and knowledgeable possession of the questioned data using various methods • follow electronic data trails to uncover links between individuals or groups • piece together strings of interactions that provide a picture of activity using evidence collected from other sources than electronic devices • perform computer network defence (CND) incident triage, to include determining scope, urgency, and potential impact; identifying the specific		

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
	vulnerability; and making recommendations that enable expeditious remediation • perform various types of forensics analysis as per the requirement of media type, data, or constraints • identify outside attackers accessing the system from the internet or insider attackers, that is, authorized users attempting to gain and misuse non-authorized privileges • follow investigation procedure in order to determine the identity of attacker **Report and present the results of a forensic investigation** • list and organise for supporting materials that are included with the report, such as printouts of particular items of evidence, digital copies of evidence, chain of custody documentation, photos, emails (showing email headers, the path and timing emails took to get from source to destination), etc. • create a brief summary of the results of the examinations performed on the items submitted for analysis		

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
	• provide comprehensive details of findings in the report • create a glossary with the report to assist the reader using an accepted source for the definition of the terms and include appropriate references • ensure that the evidence remains pristine and unaltered while presenting • present and explain track record of information exchange, and the "hash! Value", also referred to as a checksum, as a mark of authenticity • carefully document each stage of your investigation • work within the level of authority and expertise taking actions necessary should these be exceeded • differentiate between fact and opinion and express opinions within your area of expertise while writing the report •		
Professional and Technical Skills/ Expertise/ Professional Knowledge	• Common cyber security solutions • system and application security threats and vulnerabilities • networking principles • internet ports, protocols and services and their usefulness	A forensic specialist has to be an advanced expert in various areas like IT (networking, operating systems, internet, computers, and other devices); types of cyber-attacks, legal requirements; electronics; digital forensics; report writing, etc. He also needs to have a strong professional background in investigating cyber-crimes,	5.5

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
	• organization's typical patterns of usage on systems and networks • the types of operating systems and how to deal with them • knowledge of all aspects of the computer including but not limited to hard drives, networking, and encryption • types of electronic evidence, devices containing electronic evidence and external connections to such devices • possible electronic evidence sources • basic steps of the examination and analysis processes • various approaches and tools for various types of digital forensic analysis • basic concepts and practices of processing digital forensic data • comparison and evaluation methods and techniques used in forensic examinations • principles involved in processing, evaluating, and interpreting results of examinations, and the importance of considering probability and statistical variation • the established scientific and forensic principles and practices on which to base conclusions	foreseeing critical forensic testing scenarios, knowledge of all aspects of computer systems, network securities, concepts, and practices of processing digital forensic data, structuring a forensic and exhaustive steps to arrive at definite conclusions etc., hence requiring a wide range of factual, theoretical, and practical skill sets.	

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
	• approaches and techniques needed for analysing data and drawing conclusions • legal and technical limitations to various analysis approaches and techniques • the implications of current law, policies, operating procedures, and guidelines relevant to the evaluation and interpretation of forensic materials • the principal types of stakeholders and their different requirements from forensic examination processes • the type, extent, and purpose of reports regarding forensic examinations • how to assimilate different opinions and propositions in order to formulate conclusions within area of expertise • characteristics and relative value of all network traffic data sources so that relevant data can be located • processes for seizing and preserving digital evidence and maintaining chain of custody • methods of protecting and concealing electronic information including locking, encryption, sealing, etc. • how to identify and deal with protected and/or concealed systems		

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
	• the types of actions necessary to preserve third party and volatile data sources • do's and don'ts for seizing and recording electronic evidence sources • processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data • various encryption algorithms • how to take data backup or make copies of data sources, types of backups		
Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	• ensure that the scene is secured to prevent unauthorized access and alteration or damage of the evidence as per containment policies and situational considerations • identify and obtain materials related to digital communications which are relevant to the investigation • create a plan that prioritizes the sources, establishing the order in which the computing devices or records can be acquired • use forensic tools to collect volatile data • duplicate non-volatile data sources to collect their data, securing the original non-volatile data sources	The work involves identifying what could be a source of evidence, then extraction of data and analysing it and piecing together strings of such data and interactions to provide a picture of activity that can be used as evidence in a court of law. This requires demonstration of high levels of cognitive thinking, analytical mindset, and practical skills.	5.5

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
	• verify and preserve the integrity of the data source device or record in accordance with investigation procedures • carefully document each stage of the seizure and investigation • ensure chain of custody is followed for all digital media acquired in accordance with the rules of evidence • identify data that is required to be extracted and most likely sources • select the best method and tools for extraction as per the make and model of device • locate the required files and electronic data manually or using forensic tools • find, recover, and copy data from disks that may have been hidden, encrypted or damaged, etc. • perform analysis of the extracted data using various forensic tools • perform data hiding analysis for detecting and recovering data and may indicate knowledge, ownership, or intent • analyse programs and files in various ways to provide insight into the capability of the system and the knowledge of the user		

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
	• analyse file metadata typically through the application that created it to provide insight into detailed information like authorship, time last edited, number of times edited, and print or saved location, etc. • determine ownership and knowledgeable possession of the questioned data using various methods • follow electronic data trails to uncover links between individuals or groups • piece together strings of interactions that provide a picture of activity using evidence collected from other sources than electronic devices • perform computer network defence (CND) incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation • perform various types of forensics analysis as per the requirement of media type, data, or constraints • identify outside attackers accessing the system from the internet or insider attackers, that is, authorized users		

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
	attempting to gain and misuse non-authorized privileges • follow investigation procedure in order to determine the identity of attacker • provide comprehensive details of findings in the report • work within the level of authority and expertise taking actions necessary should these be exceeded • differentiate between fact and opinion and express opinions within your area of expertise while writing the report		
Broad Learning Outcomes/Core Skill	• ensure that necessary authorizations and resources are in place to conduct a forensics evidence seizure for an investigation. • ensure that the scene is physically secured to prevent unauthorized access and alteration or damage of the evidence as per containment policies and situational considerations. • carefully document each stage of the seizure and investigation • ensure chain of custody is followed for all digital media acquired in accordance with the rules of evidence. • perform analysis of the extracted data using various forensic tools • perform data hiding analysis for detecting and recovering data and may	The forensic specialist is the expert who will be responsible to ensure that the complete handling of the case from crime scene management, ensuring chain of custody is followed; seizing and transporting of evidences; examining, analyzing, and putting together complete picture and further preparing a report that can be submitted in the court of law with evidence that is in a condition that is acceptable in a court of law. Hence, some of the critical skills like logical thinking in the investigation process, mathematical skills perform decryption, decoding and forensic testing techniques and a general understanding of social and political themes to stay abreast of plausible motives and situational contexts for the cyber-attacks, are extremely crucial. There will be teams involved in the various technical functions that support the forensic	5.5

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
	indicate knowledge, ownership, or intent. • analyse programs and files in various ways to provide insight into the capability of the system and the knowledge of the user • identify any risks to safety linked to working with forensic items in line with health and safety procedures • determine ownership and knowledgeable possession of the questioned data using various methods • follow electronic data trails to uncover links between individuals or groups	specialist, however complete responsibility lies with the forensic specialist.	
Responsibility	• Responsibility of his own work and also responsible for others work and learning	There will be teams involved in the various technical functions that support the forensic specialist, however, complete responsibility lies with the forensic specialist.	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
1	PC/Laptop with internet		
2	Documentation tool	Google Docs	
3	Forensic Tool	Autopsy	
4	Network analysis tool	Wireshark	
5	Data Extraction and Backup tool	Clonezilla	

6	Cybersecurity and threat intelligence tool	MITRE Atta&ck	
7	Malware analysis tool	ClamAV	
8	Logging and analysis tools	ELK Stack	
9	Incident response tool	GNS3	

- Tools are open source

Classroom Aids

The aids required to conduct sessions in the classroom are:

1. White Board
2. White Board Marker
3. Projector

Annexure: Industry Validations Summary

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

S. No	Organization Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID	LinkedIn Profile (if available)
1	Renew	Aseem Mukhi	Chief Information Security Officer	-	9990002658	assem.mukhi@gmail.com	https://www.linkedin.com/in/aseem-mukhi-1544854/
2	Sankey Solutions	Sobha Patil	CEO	-	9008193344	shobha@sankeysolutions.com	https://www.linkedin.com/in/shobhapatil/?originalSubdomain=in
3	Accolite Digital	Ayushmaan Pandey	Senior Software Engineer	-	8077386365	ayushmaan.pandey@accolitedigital.com	https://www.linkedin.com/in/ayushmaanpandey
4	Infosys	Vivek Pilaniya	Program Manager	-	9718423687	vivek.pilania@infosys.com	https://www.linkedin.com/in/vivekpilania-iimc
5	Data Switch	Thilak Hari A	Product Engineer	-	6393798750	thilakhariharan@gmail.com	https://www.linkedin.com/in/thilak-hariharasudhan-43a89b269/

6	Forbes	Naveenkumar Janakiraman	Data Research Analyst	-	9976773109	naveenkumarj4997@gmail.com	https://www.linkedin.com/in/naveenkumar-janakiraman
7	S3V Vascular Technologies	Yeaswanth Raj V	Clinical Research Executive	-	7502629955	yeaswanthraj@gmail.com	-
8	Kornferry	Ragul Kumar	Data analyst	-	9659964881	ragul@kornferry.com	https://www.linkedin.com/in/ragul-kumar-b2297a171/
9	Acolyte	Saranya	Research Analyst	-	9944313170	saranyakathir128@gmail.com	-
10	Frontier	Santhosh kumar S	DevOps L1	-	9655747400	santhoshselvaraj24031998@gmail.com	-
11	Amazon	Asvin Ragav R	Data Associate	-	9994308478	asvinragav16@gmail.com	-
12	Rndsoft	Tamilselvan	Software developer	-	9361784871	dtamilselvan1004@gmail.com	-
13	Intellibren	Kailash PD	Director	-	6374700185	kailash@intellibren.com	-
14	Mindshare (Inclusive Minds)	Pamindar Singh	Team Lead	-	8713901984	paminder.singh@themindshare.in	https://www.linkedin.com/in/paminder-singh-7990b8101/
15	Iaccept software pvt ltd	B Mohan Kumar	Founder	-	9845208784	mohan@iaccept.in	https://www.linkedin.com/in/bmohankumar/?originalSubdomain=in
16	QAcadmey	Deepak Gour	Product and Academic Head	-	9893554394	deepak@qacademy.ca	https://ca.linkedin.com/in/deepak-gour-8853968
17	TCS	Karthiga N	Test Analyst	-	7092257551	karthiga0115@gmail.com	-
18	Skillsda	Sankar Vijyan/Thiru R	Centre Manager/Head R&D	-	9894801793	sv@skillsda.com/thiru@skillsda.com	https://www.linkedin.com/in/sankar-vijayan-73a33852/

19	Wipro	Narendra Nande	Director	-	9900086708	narendra.nande@wipro.com	https://www.linkedin.com/in/narendra-nande-84402a2/?originalSubdomain=in
20	Barq	Satheesh Sekar	Senior Decision Scientist	-	9444218513	satheeshk.sekar@gmail.com	https://www.linkedin.com/in/satheeshksekar/?originalSubdomain=in
21	Neoquant	Rishi Agrawal	Chief Technology Officer	-	7702191049	agrishi@gmail.com/Rishi.agarwal@neoquant.com	https://www.linkedin.com/in/agrishi/?originalSubdomain=in

Annexure: Training & Employment Details

Training & Employment Projections:

Year	Total Candidates		Women		People with Disability	
	Estimated Training #	Estimated Employed Opportunities	Estimated Training #	Estimated Employed Opportunities	Estimated Training #	Estimated Employed Opportunities

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

Training, Assessment, Certification, and Placement Data for previous versions of qualifications:

Qualification Version	Year	Total Candidates			Women			People with disability		
		Trained	Assessed	Certified	Trained	Assessed	Certified	Trained	Assessed	Certified

Applicable for revised qualifications only; data to be provided year-wise for the next 3 years.

List Schemes in which the previous version of qualification was implemented:

1.

Content availability for the previous version of qualifications:

☐ Participant Handbook ☐ Facilitator Guide ☐ Digital Content ☐ Qualification Handbook ☐ Any Other:

Language in which content is available:

Annexure: 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 Qualification	List Recommended Tools – for all Selected Components	Offline: Online Ratio
1	☐Theory/ Lectures - Imparting theoretical and conceptual knowledge	NA	NA
2	☐Imparting Soft Skills, Life Skills, and Employability Skills /Mentorship to Learners	NA	NA
3	☐Showing Practical Demonstrations to the learners	NA	NA
4	☐Imparting Practical Hands-on Skills/ Lab Work/ workshop/ shop floor training	NA	NA
5	☐Tutorials/ Assignments/ Drill/ Practice	NA	NA
6	☐Proctored Monitoring/ Assessment/ Evaluation/ Examinations	NA	NA
7	☐On the Job Training (OJT)/ Project Work Internship/ Candidate Training	NA	NA

Annexure: Detailed Assessment Criteria

Detailed Assessment criteria for each NOS/Module are as follows:

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
SSC/N0929 (Identify, preserve and seize digital/electronics devices or records for investigation of possible breach or crime)	PC1. Ensure necessary authorizations and resources are in place to conduct evidence seizure for an investigation	1	2	-	1
	PC2. Secure the scene physically to prevent unauthorized access or damage to potential evidence sources	1	2	-	1
	PC3. Survey the area to identify and locate potential digital evidence sources and relevant devices or records	1	2	-	1
	PC4. Identify additional data sources and their owners that can be accessed for evidence collection	1	2	-	1
	PC5. Obtain materials related to digital communications relevant to the investigation while ensuring device integrity	1	2	-	1
	PC6. Confirm that devices are operational but disconnected from networks to preserve data and prevent tampering	1	2	-	1
	PC7. Check and terminate destructive software on devices while maximizing preservation of data	1	2	-	1
	PC8. Prioritize potential data sources based on their likely value and relevance to the investigation	1	2	-	1
	PC9. Determine whether data is volatile or non-volatile to ensure proper preservation techniques	1	2	-	1
	PC10. Develop a plan to acquire data sources in a logical order based on priority and type	1	2	-	1
	PC11. Use forensic tools to collect volatile data and verify the integrity of sources throughout the process	2	3	-	1
	PC12. Record the current state and configuration of digital devices and media at the time of seizure	2	3	-	1
	PC13. Handle digital evidence carefully to preserve fingerprints, DNA, and other physical evidence as well as digital data	2	3	-	1
	PC14. Document every activity performed on devices including photographs, logs, and detailed notes for chain of custody	2	3	-	1
	PC15. Package seal and label evidence properly following forensic procedures, addressing any packaging issues	2	3	-	1

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC16. Maintain detailed logs of all steps taken including tools used and personnel involved to ensure traceability	2	3	-	1
	PC17. Transport and store evidence securely to prevent contamination, damage, or loss while following legal guidelines	2	3	-	1
	PC18. Ensure all forensic team members are trained and certified to meet legal and industry standards	2	3	-	1
	PC19. Follow legal regulations and establish procedures for collaboration with law enforcement agencies	2	3	-	1
	PC20. Maintain comprehensive case files and implement quality controls to validate findings and ensure ongoing process integrity	2	3	-	1
	Total Marks	**30**	**50**	**-**	**20**
SSC/N0930 (Extract relevant data or information from digital forensic evidence)	PC1. Obtain forensic items relevant to investigations from authorized channels in accordance with procedures and verify their accuracy against records	3	5	-	2
	PC2. Identify and prepare necessary resources and tools for extracting data from evidence devices or media	3	5	-	2
	PC3. Create a backup by making a forensic image or copy of the original storage device using clean and verified media	3	5	-	2
	PC4. Install write blocking tools to prevent any modification of the original data and select suitable extraction methods based on device type and make	3	5	-	2
	PC5. Use forensic tools and manual techniques to locate required files and data including hidden, deleted, or lost information	3	5	-	2
	PC6. Analyze slack space, encrypted data, steganography, and file headers to uncover additional or concealed information	3	5	-	2
	PC7. Crack or bypass passwords protecting files and devices using appropriate utilities and cryptographic techniques to access data	3	5	-	2
	PC8. Extract data and metadata from files and disk images, and recover information from damaged or encrypted disks while ensuring data integrity through hashing and checksums	3	5	-	2
	PC9. Document each step of the extraction process including tools used, data recovered, and any analysis performed to maintain chain of custody and procedural integrity	3	5	-	2

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC10. Collaborate with forensic specialists and stakeholders to verify findings, develop forensic timelines, and ensure compliance with data privacy and safety protocols	3	5	-	2
	Total Marks	**30**	**50**	**-**	**20**
SSC/N0931 (Analyse information or data extracted from digital forensic evidences)	PC1. Gather necessary resources and tools to support the analysis of forensic evidence and ensure all required data is available	3	5	-	2
	PC2. Use forensic tools and techniques to analyze extracted data and identify relevant insights related to the investigation	3	5	-	2
	PC3. Review time stamps, system and application logs to establish a timeline of activity and link files or events to investigation periods	3	5	-	2
	PC4. Analyze file metadata including authorship, last edited time, and save locations to gather detailed evidence context	3	5	-	2
	PC5. Assess data hiding techniques, such as steganography or concealed files, to uncover hidden information and indications of knowledge or intent	3	5	-	2
	PC6. Examine network traffic and mobile device records to identify connections, locations, and potential point of attack or breach	3	5	-	2
	PC7. Correlate evidence from various sources to reconstruct activities, identify compromised systems, and determine the scope and impact of incidents	3	5	-	2
	PC8. Use data visualization and reporting techniques to present analysis findings clearly and aid understanding among stakeholders	3	5	-	2
	PC9. Conduct interviews, gather witness statements, and review related materials to supplement digital evidence and provide additional context	3	5	-	2
	PC10. Identify elements of proof related to the crime, evaluate the effectiveness of existing security controls, and recommend improvements based on analysis results	3	5	-	2
	Total Marks	**30**	**50**	-	**20**
SSC/0932 (Report and present the results of a forensic investigation)	PC1. Obtain and organize all necessary resources and supporting materials required for drafting and presenting the forensic report	3	5	-	2
	PC2. Collate and accurately capture all relevant information and evidence findings in the report with clear documentation	3	5	-	2
	PC3. Summarize key examination results and provide comprehensive details of findings to support conclusions	3	5	-	2

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	PC4. Create an executive summary to highlight main findings and recommendations for high-level stakeholders	3	5	-	2
	PC5. Develop a glossary of terms and clearly differentiate between facts and opinions within the report to aid understanding	3	5	-	2
	PC6. Ensure evidence remains unaltered and maintains the integrity of digital evidence throughout the reporting process	3	5	-	2
	PC7. Document each stage of the investigation meticulously and include chain of custody records and supporting evidence	3	5	-	2
	PC8. Prepare and deliver an oral presentation with visual aids to effectively communicate findings to stakeholders or legal authorities	3	5	-	2
	PC9. Verify the completeness and accuracy of the report and supporting materials through review and peer validation before final submission	3	5	-	2
	PC10. Ensure secure storage and backup of all digital evidence and related documents post-reporting and maintain a record of all communications.	3	5	-	2
	Total Marks	**30**	**50**	-	**20**
DGT/VSQ/N0102 Employability Skill (60 Hours)	PC1. Introduction to Employability Skills	1	1	-	-
	PC2. Constitutional values – Citizenship	1	1	-	-
	PC3. Becoming a Professional in the 21st Century	2	4	-	-
	PC4. Basic English Skills	2	3	-	-
	PC5. Career Development & Goal Setting	1	2	-	-
	PC6. Communication Skills	2	2	-	-
	PC7. Diversity & Inclusion	1	2	-	-
	PC8. Financial and Legal Literacy	2	3	-	-
	PC9. Essential Digital Skills	3	4	-	-
	PC10. Entrepreneurship	2	3	-	-
	PC11. Customer Service	1	2	-	-
	PC12. Getting Ready for Apprenticeship & Jobs	2	3	-	-
	Total Marks	**20**	**30**	**-**	**-**
Grand Total Marks		**140**	**230**	**-**	**80**

Annexure: Assessment Strategy

Assessment Process Overview

Batch Creation & Assessment Request:

Training Providers (TP) or Training Centers (TC), including any other authorized partner of Ministry/ Department create batches / push batches on the SIDH portal. Assessment requests are submitted through the SIDH portal or via email or other media as authorized from time to time. For NON-SIDH schemes, assessment requests are received electronically or through respective State Skill Mission portals. TP/TC initiates the assessment request through the InSDMS portal and processes the payment (where applicable).

Batch Alignment & Confirmation:

Upon payment confirmation, batches are assigned to the Assessment Agency based on factors like:

- Assessment readiness
- Availability of certified assessors for the specific job role
- Assessment capping to an assessment agency as prescribed from time to time for an AB An email communication / prescribed mode communication is sent to TP/TC for confirmation of the assessment date, with IT-ITeS SSC in the loop. Once confirmation is received, the Assessment Agency designates a TOA-certified assessor to conduct or facilitate the assessment.
- Batches are only formed when the Qualification is active.

Candidate Verification & Assessment Execution:

Candidate details are verified and documented at the beginning of the assessment by a certified assessor. A Quality Assurance (QA) mechanism is enforced, requiring an undertaking from the TC. Regular feedback is collected from TP/TC to ensure continuous improvement.

Evidence Collection & Validation:

Proctors or assessors capture date/time-stamped and geo-tagged photographs of the assessment location during the process. Attendance is also ensured offline. A PC-wise result analysis is conducted to refine assessment standards.

Monitoring & Compliance:

Batch monitoring follows established protocols, ensuring adherence to assessment guidelines. Sample based surprise visits are conducted at TC locations during both training and assessments to verify compliance. This structured approach ensures transparency, quality control, and validation throughout the assessment process.

Testing Environment:

- Check the Assessment location, date and time
- If the batch size is more than 30, then there should be 2 Assessors.
- Check that the allotted time to the candidates to complete Theory & Practical Assessment is correct.

Assessment Quality Assurance levels/Framework:

IT-ITeS SSC nasscom is responsible for the development and periodic review of the question bank developed for a specific job role. We publish an openly accessible sample /model question paper on our website for all stakeholders. The quality of the Question Bank created by the assessment designer is validated by a Subject matter experts on the following parameters:

- Appropriateness of the Question Bank in terms of facts, data and information.
- Checks for grammar, spellings, scripting and formatting.
- The information provided should be specific enough to remove any ambiguity in answers/solutions to the question.
- Relevance – Assessing the topic well w.r.t. the job role.
- Check if the difficulty level of each question is as per the matrix.
- Check if the images used in the question are clear and relevant.
- All variables, symbols and abbreviations used must be declared.
- The correct answer option should be unique, and the options should not be overlapping

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 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 based on their main economic function, product, service or technology.