Model Curriculum

QP Name: Domestic Biometric Data Operator

QP Code: SSC/Q2213

Version: 4.0

NSQF Level: 3.0

Model Curriculum Version: 4.0

IT-ITeS SSC NASSCOM || NASSCOM Plot No - 7, 8, 9 & 10, 3rd Floor, Sector 126 Noida Uttar Pradesh - 201303 || email: standards@nasscom.in

Table of Contents

Contents

Training Parameters 3

Program Overview 4

Training Outcomes 4

Compulsory Modules 4

Module 1: Introduction to the IT-ITeS/BPM Industries and the job role of a Domestic Biometric Data Operator 6

Module 2: Authentication Process Verification 7

Module 3: Record-Keeping and Data Management 8

Module 4: Data Security Compliance and Secure Data Handling 9

Module 5: Risk Management, Data Integrity, and Stakeholder Collaboration 10

Module 6: Employability Skills (30 Hours) 12

Module 7: On-the-Job Training 14

Annexure 15

Trainer Requirements 15

Assessor Requirements 16

Assessment Strategy 17

Glossary 19

Acronyms and Abbreviations 20

Training Parameters

Sector	IT-ITeS
Sub-Sector	Business Process Management
Occupation	Customer Relationship Management (CRM)
Country	India
NSQF Level	3
Aligned to NCO/ISCO/ISIC Code	NCO-2015/3511.0101
Minimum Educational Qualification and Experience	Grade 10 OR 8th Grade Pass with 1.5-year relevant experience* *Relevant Experience: Computer Service domain The relevant experience would include work, internship, and apprenticeship after completing relevant educational qualifications.
Pre-Requisite License or Training	NA
Last Reviewed On	18-02-2025
Next Review Date	18-02-2028
NSQC Approval Date	18-02-2025
QP Version	4.0
Model Curriculum Creation Date	18-02-2025
Model Curriculum Valid Up to Date	18-02-2028
Model Curriculum Version	4.0
Minimum Duration of the Course	360 Hours
Maximum Duration of the Course	360 Hours

Program Overview

This section summarises the end objectives of the program along with its duration.

Training Outcomes

At the end of the program, the learner should have acquired the listed knowledge and skills to:

- Explain the process of collecting biometric data and creating biometric templates.
- Discuss the steps involved in undertaking biometric data authentication and entry.
- Explain the data security and privacy management for data handling roles.
- Elucidate the Employability Skills required for jobs in various industries.

Compulsory Modules

The table lists the modules and their duration corresponding to the Compulsory NOS of the QP.

NOS and Module Details	Theory Duration (Hours)	Practical Duration (Hours)	On-the-Job Training Duration (Mandatory) (Hours)	On-the-Job Training Duration (Recommended) (Hours)	Total Duration (Hours)
SSC/N3023: Undertake Bio-Metric data entry and processing **NOS Version No.: 3.0** **NSQF Level: 3.0**	**60:00**	**120:00**	**60:00**	**00:00**	**240:00**
Module 1: Introduction to the IT-ITeS/BPM Industry and the job role of a Domestic Biometric Data Operator	05:00	00:00	00:00	00:00	05:00
Module 2: Authentication Process Verification	30:00	60:00	30:00	00:00	120:00
Module 3: Record-Keeping and Data Management	25:00	60:00	30:00	00:00	115:00
SSC/N2208: Data Security and Privacy Management for Data Handling Roles **NOS Version No.: 1.0** **NSQF Level: 3.0**	**30:00**	**60:00**	**00:00**	**00:00**	**90:00**
Module 4: Data Security Compliance and Secure Data Handling	10:00	20:00	00:00	00:00	30:00
Module 5: Risk Management, Data Integrity, and Stakeholder Collaboration	20:00	40:00	00:00	00:00	60:00
DGT/VSQ/N0101: Employability Skills (30 Hours) **NOS Version No.: 1.0**	**30:00**	**00:00**	**00:00**	**00:00**	**30:00**

NSQF Level: 2.0					
Module 6: Employability Skills (30 Hours)	30:00	00:00	00:00	00:00	30:00
Total Duration	**120:00**	**180:00**	**60:00**	**00:00**	**360:00**

Module Details

Module 1: Introduction to the IT-ITeS/BPM Industries and the job role of a Domestic Biometric Data Operator

Mapped to SSC/N3023, v3.0

Terminal Outcomes:

- Explain the importance of IT-ITeS/BPM Industries.
- Discuss the roles and responsibilities of a Domestic Biometric Data Operator.

Duration (in hours): 05:00	**Duration (in hours): 00:00**
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Define the ITeS/BPM industry. • Describe the various sub-sectors within the ITeS/BPM industry. • Discuss the scope of employment in the ITeS/BPM industry. • Describe the roles and responsibilities of a Domestic Biometric Data Operator. • Discuss the future trends and career growth opportunities for a Domestic Biometric Data Operator.	-
Classroom Aids	
Training Kit - Facilitator's Guide, Participant's Handbook, Presentations and Software, Whiteboard, Marker, Projector, Laptop, Video Films	
Tools, Equipment and Other Requirements	
Nil	

Module 2: Authentication Process Verification

Mapped to SSC/N3023, v1.0

Terminal Outcomes:

- Explain the process of authentication in a biometric system.

Duration (in hours): 30:00	Duration (in hours): 60:00
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the appropriate biometric data entry procedures, tools, and techniques for accurate data capture and entry. • Discuss the requirements of typical helpdesk customers and the tools used for incident management and customer support in biometric systems. • Describe the criteria distinguishing acceptable vs. non-acceptable biometric data according to standards and policies. • Explain the basic computer configuration, networking, and maintenance requirements for biometric data capture and processing. • Elucidate the principles of biometric system error rates, including false accept, false reject, equal error rate, and detection error trade-off.	• Demonstrate how to capture the biometric data of target users through data collection and processing, including face recognition and iris scanning, while adhering to established guidelines. • Show how to establish a user's identity by matching the captured biometric data with the stored data in the system. • Demonstrate how to validate biometric data by verifying its accuracy and completeness during data collection and processing. • Demonstrate how to grant access to users based on the successful match of their biometric data with the system's records. • Show how to ensure users are informed about the guidelines for accessing and using the relevant facility or system. • Demonstrate how to identify and handle exceptions to ensure the smooth operation of the biometric system. • Show how to coordinate with the biometric equipment manufacturer to resolve complex issues with the biometrics system.
Classroom Aids	
Training Kit - Facilitator's Guide, Participant's Handbook, Presentations and Software, Whiteboard, Marker, Projector, Laptop, Video Films	
Tools, Equipment and Other Requirements	
Fingerprint Scanners, Facial Recognition Cameras,	

Module 3: Record-Keeping and Data Management

Mapped to SSC/N3023, v1.0

Terminal Outcomes:

- Describe how to maintain appropriate records in a biometric data system.

Duration (in hours): 25:00	Duration (in hours): 60:00
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain procedures for compiling reports and making data comparisons using database management software. • Discuss the importance of documenting, classifying, and prioritizing service requests. • Describe the process for registering and securely capturing biometric data. • Elucidate encryption methods like hashing and salting to secure biometric data. • Determine factors affecting the accuracy and reliability of biometric sensors. • Explain the difference between one-to-one and one-to-many biometric matching algorithms. • Discuss biometric codes and standards, including data protection laws. • Describe biometric authentication in physical and logical control systems, and relevant performance metrics.	• Demonstrate how to log biometric data transactions for auditing purposes. • Show how to collect and enter data from handwritten applications of individuals into the appropriate computer program. • Demonstrate how to review and verify the captured biometric data for accuracy. • Show how to compare the transcribed data with the source document and correct any errors, with the supervisor's help if required. • Demonstrate how to manage errors in biometric face recognition or iris scanning by adhering to SOP guidelines and maintaining compliance with security protocols. • Show how to ensure all biometric documentation is complete while maintaining data privacy and security. • Demonstrate how to maintain data back-ups to prevent the accidental loss of biometric data. • Show how to ensure compliance with relevant privacy and security laws and regulations governing biometric data collection and storage.
Classroom Aids	
Training Kit - Facilitator's Guide, Participant's Handbook, Presentations and Software, Whiteboard, Marker, Projector, Laptop, Video Films	
Tools, Equipment and Other Requirements	
Fingerprint Scanners, Facial Recognition Cameras,	

Module 4: Data Security Compliance and Secure Data Handling

Mapped to SSC/N2208, v1.0

Terminal Outcomes:

- Explain how compliance with data security and privacy regulations can be ensured in an organization.
- Discuss strategies to secure data collection, storage, and transmission effectively.

Duration (in hours): 10:00	Duration (in hours): 20:00
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the legal and regulatory requirements for data security, privacy, and compliance, including GDPR, CCPA, and other regional laws. • Discuss best practices for encrypting data at rest, in transit, and during collection. • Describe methods for implementing role-based access control (RBAC) and the principle of least privilege. • Determine authentication methods such as passwords, biometrics, multi-factor authentication (MFA), and token-based authentication. • Discuss strategies for monitoring and logging system access, data changes, and user activities to detect security threats. • Explain methods for securing sensitive data during storage and transmission, including cloud environments. • Discuss best practices for managing data retention, disposal, and anonymization in compliance with legal and organizational requirements.	• Demonstrate how to follow applicable data privacy laws and organizational data security policies. • Show how to verify compliance through audits, assessments, and regular reviews. • Demonstrate how to ensure the collection, storage, and transmission of sensitive data is encrypted and securely handled. • Show how to apply access controls to data storage and ensure only authorized personnel have access. • Demonstrate how to verify secure transmission protocols to prevent unauthorized access during data transfer.
Classroom Aids	
Training Kit - Facilitator's Guide, Participant's Handbook, Presentations and Software, Whiteboard, Marker, Projector, Laptop, Video Films	
Tools, Equipment and Other Requirements	
Access Management Systems for Data Security (e.g. OpenLDAP, FreeIPA, Keycloak, etc.)	

Module 5: Risk Management, Data Integrity, and Stakeholder Collaboration

Mapped to SSC/N2208, v1.0

Terminal Outcomes:

- Describe the process of implementing access controls and authentication mechanisms to enhance data security.
- Determine methods to identify and mitigate potential data security risks effectively.
- Explain how to ensure data integrity and availability in a secure environment.
- Discuss best practices for secure data disposal and archiving.
- Elucidate how collaboration with relevant stakeholders contributes to maintaining security standards.

Duration (in hours): 20:00	Duration (in hours): 40:00
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Elucidate techniques for identifying, assessing, and mitigating risks like malware, phishing, and insider threats. • Explain response protocols for handling data breaches, including containment, notification, and reporting. • Discuss approaches for conducting vulnerability assessments and penetration testing to identify and address system weaknesses. • Describe the principles of data integrity to ensure the reliability and accuracy of data throughout its lifecycle. • Discuss disaster recovery strategies to ensure data availability and business continuity in the event of data loss or breach. • Determine tools and technologies used in data security, such as encryption software, firewalls, antivirus software, and intrusion detection systems. • Discuss emerging trends in data security, such as AI and machine learning-driven threats. • Describe the roles and responsibilities of data protection officers (DPOs), IT security teams, and compliance officers in maintaining data privacy and security.	• Demonstrate how to set up role-based access control (RBAC) and enforce multi-factor authentication (MFA) for system access. • Show how to regularly monitor and review access logs for suspicious activities and potential security threats. • Demonstrate how to assess potential risks related to data security, including malware, insider threats, and external attacks. • Show how to implement proactive measures and technologies to mitigate identified security risks. • Demonstrate how to implement data backup, disaster recovery, and availability strategies to ensure business continuity. • Show how to protect data from unauthorized alteration or corruption by using encryption and validation mechanisms. • Demonstrate how to securely dispose of or anonymize data that is no longer needed or legally required. • Show how to apply secure deletion methods to remove sensitive data from storage and systems when no longer required. • Demonstrate how to work with IT security, legal, and compliance teams to implement and maintain security

	measures. • Show how to communicate security policies and procedures effectively to all relevant personnel within the organization.
Classroom Aids	
Training Kit - Facilitator's Guide, Participant's Handbook, Presentations and Software, Whiteboard, Marker, Projector, Laptop, Video Films	
Tools, Equipment and Other Requirements	
Risk Assessment Tools (e.g. OpenVAS, Nikto, etc.), Intrusion Detection and Prevention Systems (IDPS) (e.g. Snort)	

Module 6: Employability Skills (30 Hours)

Mapped to DGT/VSQ/N0101, v1.0

Duration: 30:00 Hours

Key Learning Outcomes

Introduction to Employability Skills Duration: 1 Hour

After completing this programme, participants will be able to:

1. Discuss the importance of Employability Skills in meeting the job requirements

Constitutional values - Citizenship Duration: 1 Hour

2. Explain constitutional values, civic rights, duties, citizenship, responsibility towards society etc. that are required to be followed to become a responsible citizen.

3. Show how to practice different environmentally sustainable practices

Becoming a Professional in the 21st Century Duration: 1 Hour

4. Discuss 21st-century skills.

5. Display a positive attitude, self-motivation, problem-solving, time management skills and continuous learning mindset in different situations.

Basic English Skills Duration: 2 Hours

6. Use appropriate basic English sentences/phrases while speaking

Communication Skills Duration: 4 Hours

7. Demonstrate how to communicate in a well-mannered way with others.

8. Demonstrate working with others in a team

Diversity & Inclusion Duration: 1 Hour

9. Show how to conduct oneself appropriately with all genders and PwD

10. Discuss the significance of reporting sexual harassment issues in time

Financial and Legal Literacy Duration: 4 Hours

11. Discuss the significance of using financial products and services safely and securely.

12. Explain the importance of managing expenses, income, and savings.

13. Explain the significance of approaching the concerned authorities in time for any exploitation as per legal rights and laws

Essential Digital Skills Duration: 3 Hours

14. Show how to operate digital devices and use the associated applications and features, safely and securely

15. Discuss the significance of using the internet for browsing, and accessing social media platforms, safely and securely

Entrepreneurship Duration: 7 Hours

16. Discuss the need for identifying opportunities for potential business, sources for arranging money and potential legal and financial challenges

Customer Service Duration: 4 Hours

17. Differentiate between types of customers

18. Explain the significance of identifying customer needs and addressing them

19. Discuss the significance of maintaining hygiene and dressing appropriately

Getting ready for Apprenticeship & Jobs Duration: 2 Hours

20. Create a biodata

21. Use various sources to search and apply for jobs

22. Discuss the significance of dressing up neatly and maintaining hygiene for an interview

23. Discuss how to search and register for apprenticeship opportunities

Module 7: On-the-Job Training

Mapped to Domestic Biometric Data Operator

Mandatory Duration (in hours): 60:00	Recommended Duration (in hours): 00:00
Location: On-Site	
Terminal Outcomes • Show how to create and store biometric templates securely. • Demonstrate the process of authentication in a biometric system. • Show how to maintain appropriate records in a biometric data system. • Demonstrate the process of data security and privacy management for data handling roles. • Show how to integrate and manage BPM platforms in biometric data processing.	

Annexure

Trainer Requirements

1.	**Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	**Educational Qualification:** Graduate in any discipline **Industry & Training Experience:** 2 years of industry experience in customer support roles **Certification:** "Trainer" mapped to the Qualification Pack "MEP/Q2602 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 in any discipline **Industry & Training Experience:** 4 years of industry experience in customer support roles **Certification:**" Master Trainer" mapped to the Qualification Pack "MEP/Q2602" Minimum accepted score is 90% aggregate.
3.	**Tools and Equipment Required for Training**	☒Yes ☐No (*If "Yes", details to be provided in Annexure)*
4.	**In Case of Revised Qualification, Details of Any Upskilling Required for Trainer**	NA

Assessor Requirements

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	**Educational Qualification:** Graduate in any discipline, **Industry & Training Experience:** 2 years of industry experience in customer support roles **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 in any discipline, **Industry & Training Experience:** 2 years of industry experience in customer support roles **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 in any discipline **Industry & Training Experience:** 4 years of industry experience in customer support roles **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)*

Assessment Strategy

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

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

References

Glossary

Term	Description
Declarative Knowledge	Declarative knowledge refers to facts, concepts and principles that need to be known and/or understood in order to accomplish a task or to solve a problem.
Key Learning Outcome	Key learning outcome is the statement of what a learner needs to know, understand and be able to do in order to achieve the terminal outcomes. A set of key learning outcomes will make up the training outcomes. Training outcome is specified in terms of knowledge, understanding (theory) and skills (practical application).
OJT (M)	On-the-job training (Mandatory); trainees are mandated to complete specified hours of training on site
OJT (R)	On-the-job training (Recommended); trainees are recommended the specified hours of training on site
Procedural Knowledge	Procedural knowledge addresses how to do something, or how to perform a task. It is the ability to work, or produce a tangible work output by applying cognitive, affective, or psychomotor skills.
Training Outcome	Training outcome is a statement of what a learner will know, understand and be able to do it upon the completion of the training.
Terminal Outcome	Terminal outcome is a statement of what a learner will know, understand and be able to do upon the completion of a module. A set of terminal outcomes help to achieve the training outcome.

Acronyms and Abbreviations

Term	Description
NCVET	National Council for Vocational Education and Training
QP	Qualification Pack
MC	Model Curriculum
NSQF	National Skills Qualification Framework
NSQC	National Skills Qualification Committee
NOS	National Occupational Standards
NCO	National Classification of Occupations
ES	Employability Skills
OJT	On the Job Training
NASSCOM	National Association of Software and Service Companies
IT-ITeS	Information Technology and Information Technology Enabled Services
IT	Information Technology
CRM	Customer Relationship Management
RBAC	Role-Based Access Control
MFA	Multi-Factor Authentication