Model Curriculum

QP Name: Analyst Endpoint Security

QP Code: SSC/Q0905

QP Version: 2.0

NSQF Level: 7

Model Curriculum Version: 1.0

IT-ITeS Sector Skill Council || IT-ITeS Sector Skill Council, NASSCOM, Plot No - 7, 8, 9 & 10, 3rd Floor, Sector 126, Noida
Uttar Pradesh – 201303

Table of Contents

Training Parameters

Sector	**IT-ITeS**
Sub-Sector	**IT Services**
Occupation	**Cyber Security**
Country	**India**
NSQF Level	**7**
Aligned to NCO/ISCO/ISIC Code	**NCO-2015/NIL**
Minimum Educational Qualification and Experience	**Diploma (IT/Computer) with 0-6 Months of full-time work experience in Information/ Cybersecurity. The full-time experience would include work, internship and apprenticeship undertaken post completion of diploma.**
Pre-Requisite License or Training	**NA**
Minimum Job Entry Age	**18 years**
Last Reviewed On	**19/06/2020**
Next Review Date	**19/06/2025**
NSQC Approval Date	**TBD**
QP Version	**2.0**
Model Curriculum Creation Date	**19/06/2020**
Model Curriculum Valid Up to Date	**19/06/2025**
Model Curriculum Version	**1.0**
Minimum Duration of the Course	**228 hours**
Maximum Duration of the Course	**228 hours**

Program Overview

This section summarizes 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:

- Explain the use cases, common roles and basic operating procedures followed by organizations in the context of cybersecurity
- Describe the security threats associated with network and ICT devices, and commonly used security solutions
- Evaluate the fundamentals of programming with respect to reading and writing scripts
- Assess various techniques for safeguarding networks and endpoint devices
- Recommend endpoint security solutions (if needed) by analysing existing systems
- Troubleshoot and maintain endpoint security in an enterprise environment
- Assist in the installation of endpoint security measures
- Plan one's schedules and timelines based on the nature of work.
- Demonstrate how to communicate and work effectively with colleagues
- Use different approaches to effectively manage and share data and information
- Identify best practices to maintain an inclusive, environmentally sustainable workplace

Compulsory Modules

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

NOS and Module Details	Theory Duration	Practical Duration	On-the-Job Training Duration (Mandatory)	On-the-Job Training Duration (Recommended)	Total Duration
Module 1 (Bridge Module): Introduction to Information/ Cyber Security	08:00	04:00	00:00	00:00	12:00
Module 2 (Bridge Module): Fundamental Concepts in Cyber Security	12:00	08:00	00:00	00:00	20:00
Module 3 (Bridge Module): Programming and Scripting	12:00	24:00	00:00	00:00	36:00
Module 4 (Bridge Module): Basics of Safeguarding Resources	16:00	08:00	00:00	00:00	24:00
SSC/N0912 – Troubleshoot and maintain endpoint security in an enterprise environment **NOS Version No. 1** **NSQF Level 7**	**20:00**	**28:00**	**00:00**	**00:00**	**48:00**
Module 5: Basics of Endpoint Security System	12:00	12:00	00:00	00:00	24:00
Module 6: Endpoint Security Maintenance	08:00	16:00	00:00	00:00	24:00

SSC/N0913 – Assist in the installation of endpoint security measures NOS Version No. 1 NSQF Level 7	**08:00**	**20:00**	**00:00**	**00:00**	**28:00**
Module 7: Lab Installation	08:00	20:00	00:00	00:00	28:00
SSC/N9001 – Manage your work to meet requirements NOS Version No. 2 NSQF Level 4	**04:00**	**08:00**	**00:00**	**00:00**	**12:00**
Module 8: Manage Your Work to Meet Requirements	04:00	08:00	00:00	00:00	12:00
SSC/N9002 - Work effectively with colleagues NOS Version No. 2 NSQF Level 4	**04:00**	**08:00**	**00:00**	**00:00**	**12:00**
Module 9: Working with Colleagues	04:00	08:00	00:00	00:00	12:00
SSC/N9004 - Provide data/information in standard formats NOS Version No. 2 NSQF Level 4	**08:00**	**16:00**	**00:00**	**00:00**	**24:00**
Module 10: Provide Data / Information in Standard Formats	08:00	16:00	00:00	00:00	24:00
SSC/N9014 – Maintain an inclusive, environmentally sustainable workplace NOS Version No. 1 NSQF Level 4	**04:00**	**08:00**	**00:00**	**00:00**	**12:00**
Module 11: Maintain an inclusive, environmentally sustainable workplace	04:00	08:00	00:00	00:00	12:00
Total Duration	**96:00**	**132:00**	**00:00**	**00:00**	**228:00**

Module Details

Module 1: Introduction to Information/Cyber Security

Bridge Module

Terminal Outcomes:

- Explain the relevance of cybersecurity in the context of evolving cyber threats
- Describe common roles in cybersecurity and basic operating procedures followed by the organizations

Duration: *08:00*	**Duration**: *04:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the relevance of Cyber Security to the society • Explain the various use-cases of Cyber Security in the industry • Explain various cyber threats associated with networks, devices and remote access technologies • Describe the responsibilities of various roles in cybersecurity, especially those specific to the role under consideration (i.e., Analyst Endpoint Security) • Describe the fundamentals of operating procedure in organizations including SLA's, data integrity & confidentiality, information recording, reporting, compliance requirements, and scope of devices/tools, stakeholders, authorizing personnel, etc.	• Create a career map for roles in Information/Cyber Security • Demonstrate the working mechanism of malicious codes such as virus, malware, logic bomb, ransomware, spyware, phishing, trojan, etc.
Classroom Aids:	
Whiteboard and markers Chart paper and sketch pens LCD Projector and Laptop for presentations	
Tools, Equipment and Other Requirements	
Labs equipped with the following: • PCs/Laptops • Internet with Wi-Fi (Min. 2 Mbps dedicated) • Samples of the templates and checklists used in organizations	

Module 2: Fundamental Concepts in Cyber Security

Bridge Module

Terminal Outcomes:

- Explain commonly used ICT devices and the associated threats
- Apply various networking concepts and commonly used security solutions

Duration: *12:00*	**Duration**: *08:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe commonly used ICT devices as well as web servers and web applications • Explain relevant networking fundamentals: – networking concepts: load balancing, OSI, Model/topology, TLS, SSL, etc – protocols: TCP/IP, FTP, SFTP, SNMP, SSH, SSL, VPN, RDP, HTTPS etc – devices: switches, routers, servers, transmission media, etc • Explain the stages of cyberattack from reconnaissance to identification and prevention • Discuss commonly used unix/windows security commands • Explain common security solutions such as firewall, intrusion detection or prevention systems (IDS/IPS), anti-virus, web security gateways, email security, etc.	• Demonstrate the use of various Network Protocols and bandwidth management tools • Demonstrate the application of host network access controls; hubs; switches; routers; bridges; servers; transmission media IDS/IPS; application of SSL, VPN, 2FA, Encryption, etc. • Demonstrate commonly used methods of data theft and unauthorized access • Demonstrate the usage of basic methods/tools in preventing cyber attacks
Classroom Aids:	
Whiteboard and markers LCD Projector and Laptop for presentations	
Tools, Equipment and Other Requirements	
Labs equipped with the following: • PCs/Laptops • Internet with Wi-Fi (Min. 2 Mbps dedicated) • Samples of the templates and checklists used in organizations	

Module 3: Programming and Scripting

Bridge Module

Terminal Outcomes:

- Evaluate various object-oriented and dynamic programming concepts
- Evaluate the fundamentals of programming with respect to reading and writing scripts

Duration: *12:00*	**Duration:** *24:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Distinguish between the limitations of different programming, command line or scripting languages such as C/C++, Java, and JavaScript programming to read and write coded scripts	• Demonstrate the ways to read and write coded scripts • Demonstrate the methods to modify and debug programs • Apply the most suitable programming languages to modify and debug programs
Classroom Aids:	
Whiteboard and markers Chart paper and sketch pens LCD Projector and Laptop for presentations	
Tools, Equipment and Other Requirements	
Labs equipped with the following: • PCs/Laptops • Internet with Wi-Fi (Min. 2 Mbps dedicated)	

Module 4: Basics of Safeguarding Resources

Bridge Module

Terminal Outcomes:

- Assess various techniques for safeguarding networks and endpoint devices

Duration: *16:00*	**Duration**: *08:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Discuss the common attack paths for threat vectors • Explain various protection techniques including network security methodologies (esp., firewall configuration), encryption, mobile phone hardening, etc. • Discuss the importance of patch management against ever-evolving cyber threats • Explain different techniques for maintaining password security against emerging attacks • Discuss the importance of cloud security and suggest solutions for cloud security maintenance	• Demonstrate the safeguarding techniques for endpoint devices
Classroom Aids:	
Whiteboard and markers LCD Projector and Laptop for presentations	
Tools, Equipment and Other Requirements	
Labs equipped with the following: • PCs/Laptops • Internet with Wi-Fi (Min. 2 Mbps dedicated)	

Module 5: Basics of Endpoint Security Systems

Mapped to SSC/N0912 (Version 1)

Terminal Outcomes:

- Demonstrate the functionality of endpoint security platforms
- Recommend endpoint security solutions (if needed) by analysing existing systems

Duration: *12:00*	**Duration**: *12:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Discuss the scope of endpoint devices in context of cybersecurity • Describe the working mechanism of an endpoint security platform • Explain client-server model and SaaS model in the context of endpoint security systems • Explain the difference in traditional and continuous endpoint security compliance models for building a robust security posture • Discuss different endpoint solutions available in the market	• Carry out configuration reviews of Endpoint systems • Demonstrate methods to analyse a set of end-point system sample for maturity of endpoint security, and recommend suitable security solutions
Classroom Aids:	
Whiteboard and markers LCD Projector and Laptop for presentations	
Tools, Equipment and Other Requirements	
Labs equipped with the following: • PCs/Laptops • Internet with Wi-Fi (Min. 2 Mbps dedicated) • Samples of secure and unsecured devices for endpoint security testing activities Tools and Programming Languages: • Scanning tools like sqlmap, OpenVAS, etc. • Firewall management suits like Redseal, Tufin, AlgoSec, etc. • Encryption tools such as GnuPG, VeraCrypt, LUKS, 7Zip, etc. • Programming Languages for mobile/app hardening such as Kotlin, C#,	

Module 6: Maintaining Endpoint Security

Mapped to SSC/N0912 (Version 1)

Terminal Outcomes:

- Explain the tools and techniques to monitor endpoint protection
- Explain how to configure and upgrade endpoint security management tools

Duration: *08:00*	**Duration**: *16:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the commonly used tools to monitor endpoint protection and detect anomalies • Explain how to distinguish between genuine security events and false positives • Discuss the methods to remediate security events or failures	• Demonstrate the functionalities of endpoint security management tools • Demonstrate the usage of logs and reports from endpoint security tools • Demonstrate analysis of sample data to identify security events • Demonstrate ways to resolve security incidents or client installation failures • Demonstrate the use of basic monitoring and troubleshooting tools • Demonstrate the configuration and upgradation of endpoint security environment and clients • Demonstrate ways to optimize the deployment manager
Classroom Aids:	
Whiteboard and markers LCD Projector and Laptop for presentations	
Tools, Equipment and Other Requirements	
Labs equipped with the following: • PCs/Laptops • Internet with Wi-Fi (Min. 2 Mbps dedicated) • Samples of secure and unsecured devices for endpoint security testing activities Tools and Programming Languages: • Scanning tools like sqlmap, OpenVAS, etc. • Commonly used end-point security software such as EnCase, Tripwire, McAffee, etc.	

Module 7: Lab Installation

Mapped to SSC/N0913 (Version 1)

Terminal Outcomes:

- Explain the installation of endpoint security products as well as endpoint security console management

Duration: *08:00*	**Duration**: *20:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe the objective, scope and specifications of endpoint security product • Explain the difference between client mode and user mode • Document the process involved in the installation and configuration of security software	• Demonstrate the process of installing management consoles on a server • Demonstrate installation of consoles and integration with Lightweight Directory Access Protocol (LDAP) and activation • Demonstrate how to configure Linux/ windows clients, unmanaged detectors, endpoint security replications, load balancing and failover • Demonstrate the creation and management of administrator accounts in Endpoint Security Manager Console • Demonstrate the installation of software on client devices across networks • Demonstrate how to configure devices for Secure Socket Layer (SSL) communications and auto-update of software and virus definition
Classroom Aids:	
Whiteboard and markers LCD Projector and Laptop for presentations	
Tools, Equipment and Other Requirements	
Labs equipped with the following: • PCs/Laptops • Internet with Wi-Fi (Min. 2 Mbps dedicated) • Samples of secure and unsecured devices for endpoint security testing activities Tools and Programming Languages: • Scanning tools like sqlmap, OpenVAS, etc. • Commonly used end-point security software such as EnCase, Tripwire, McAffee, etc.	

Module 8: Manage and Plan Work Requirements

Mapped to SSC/N9001 (Version 2)

Terminal Outcomes:

- Define the scope of work
- Demonstrate effective work planning principles
- Recognize the importance of using time and resources efficiently

Duration: *04:00*	**Duration:** *08:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Discuss the role, responsibilities & limits of the responsibilities • Discuss the importance of gathering detailed work requirements and work area prioritization • Describe the organizational guidelines and policies • Identify commonly made mistakes in the prioritized work areas • Explain the importance of accuracy in completion of work	• Analyse needs, requirements and dependencies to meet the work requirements • Apply resource management principles and techniques • Demonstrate ways to maintain an organized work area • Apply effective time management principles
Classroom Aids:	
Whiteboard and markers Chart paper and sketch pens LCD Projector and Laptop for presentations	
Tools, Equipment and Other Requirements	
Labs equipped with the following: PCs/Laptops Internet with Wi-Fi (Min. 2 Mbps dedicated)	

Module 9: Communication and Collaboration with Colleagues

Mapped to SSC/N9002 (Version 2)

Terminal Outcomes:

- Explain the methods and mechanisms for effective communication
- Explain the importance of constructive collaboration at workplace

Duration: *04:00*	**Duration**: *08:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the principles of clear communication • Outline the importance of being a good listener and adhering to the commitments • Identify challenges and pain points related to teamwork distribution • Explain the importance of distributing and sharing workloads	• Use oral, written and non-verbal communication skills in a variety of forms to construct thoughts and ideas effectively • Demonstrate professional behaviour at workplace • Demonstrate effective team mentorship
Classroom Aids:	
Whiteboard and markers Chart paper and sketch pens LCD Projector and Laptop for presentations	
Tools, Equipment and Other Requirements	
Labs equipped with the following: PCs/Laptops Internet with Wi-Fi (Min. 2 Mbps dedicated)	

Module 10: Workplace Data Management

Mapped to SSC/N9004 (Version 2)

Terminal Outcomes:

- Describe the standard formats to manage data/information accurately

Duration: *08:00*	**Duration**: *16:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Discuss data privacy in terms of sharing and retrieving data from different sources • Discuss the significance of providing accurate and timely up-to-date information • Describe commonly used database management tools and the importance of CRM database	• Apply the concepts behind information and knowledge management • Perform rule-based analysis of data/information • Format the data/information into required types/forms • Demonstrate the methods of effective data management • Use CRM databases to record and extract information
Classroom Aids:	
Whiteboard and markers Chart paper and sketch pens LCD Projector and Laptop for presentations	
Tools, Equipment and Other Requirements	
Labs equipped with the following: PCs/Laptops Internet with Wi-Fi (Min. 2 Mbps dedicated)	

Module 11: Inclusive and Environmentally Sustainable Workplaces

Mapped to SSC/N9014 (Version 1)

Terminal Outcomes:

- Illustrate sustainable practices at workplace for energy efficiency and waste management
- Apply different approaches to maintain gender equality and increase inclusiveness for PwD

Duration: *04:00*	**Duration**: *08:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe different approaches for resourceful energy utilisation and waste management • Describe the importance of following the diversity policies • Identify stereotypes and prejudices associated with differently abled people and its negative consequences • Discuss the importance of promoting, sharing and implementing gender equality and PwD sensitivity guidelines at organization level	• Practice the segregation of recyclable, non-recyclable and hazardous waste generated • Demonstrate different methods of energy resource use optimization and conservation • Demonstrate essential communication methods in line with gender inclusiveness and PwD sensitivity
Classroom Aids:	
Whiteboard and markers Chart paper and sketch pens LCD Projector and Laptop for presentations	
Tools, Equipment and Other Requirements	
Labs equipped with the following: PCs/Laptops Internet with Wi-Fi (Min. 2 Mbps dedicated)	

Annexure

Trainer Requirements

Trainer Prerequisites						
Minimum Educational Qualification	**Specialization**	**Relevant Industry Experience**		**Training Experience**		**Remarks**
		Years	***Specialization***	***Years***	***Specialization***	
Diploma	IT/ Computer	1-2 years of full-time work experience	The full-time experience would include work, internship and apprenticeship undertaken post completion of diploma	1-2 years of full-time work experience		

Trainer Certification	
Domain Certification	**Platform Certification**
Certified for Job Role: "Analyst Endpoint Security" mapped to QP: "SSC/Q0905, V2.0". Minimum accepted score is 80%	Recommended that the trainer is certified for the Job role "Trainer" mapped to the Qualification Pack "MEP/Q2601". Minimum accepted score is 80% aggregate

Assessor Requirements

Assessor Prerequisites						
Minimum Educational Qualification	**Specialization**	**Relevant Industry Experience**		**Training Experience**		**Remarks**
		Years	***Specialization***	***Years***	***Specialization***	
Diploma	IT/ Computer	1-2 years of full-time work experience	The full-time experience would include work, internship and apprenticeship undertaken post completion of diploma	1-2 years of full-time work experience		

Assessor Certification	
Domain Certification	**Platform Certification**
Certified for Job Role: "Analyst Endpoint Security" mapped to QP: "SSC/Q0905, V2.0". Minimum accepted score is 80%	Recommended that the trainer is certified for the Job role "Assessor" mapped to the Qualification Pack "MEP/Q2701". Minimum accepted score is 80% aggregate

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.

Assessment System Overview

A uniform assessment of job candidates as per industry standards facilitates progress of the industry by filtering employable individuals while simultaneously providing candidates with an analysis of personal strengths and weaknesses.

Assessment Criteria

Criteria for assessment for each Qualification Pack will be created by the Sector Skill Council (SSC). Each Performance Criteria (PC) will be assigned marks proportional to its importance in NOS. SSC will also lay down the proportion of marks for Theory and Skills Practical for each PC.

The assessment for the theory part will be based on a knowledge bank of questions created by the SSC. Assessment will be conducted for all compulsory NOS, and where applicable, on the selected elective/option NOS/set of NOS.

Guidelines for Assessment			
Testing Environment	**Tasks and Functions**	**Productivity**	**Teamwork**
• Carry out assessments under realistic work pressures that are found in the normal industry workplace (or simulated workplace). • Ensure that the range of materials, equipment and tools that learners use are current and of the type routinely found in the normal industry workplace (or simulated workplace) environments.	• Assess that all tasks and functions are completed in a way, and to a timescale, that is acceptable in the normal industry workplace. • Assign workplace (or simulated workplace) responsibilities that enable learners to meet the requirements of the NOS.	• Productivity levels must be checked to ensure that it reflects those that are found in the work situation being replicated.	• Provide situations that allow learners to interact with the range of personnel and contractors found in the normal industry workplace (or simulated workplace).

Assessment Quality Assurance framework

NASSCOM provides two assessment frameworks NAC and NAC-Tech.

NAC (NASSCOM Assessment of Competence)

NAC follows a test matrix to assess Speaking & Listening, Analytical, Quantitative, Writing, and Keyboard skills of candidates appearing for assessment.

NAC-Tech

NAC-Tech test matrix includes assessment of Communication, Reading, Analytical, Logical Reasoning, Work Management, Computer Fundamentals, Operating Systems, RDBMS, SDLC, Algorithms & Programming Fundamentals, and System Architecture skills.

Methods of Validation

To pass a QP, a trainee should score an average of 70% across generic NOS' and a minimum of 70% for each technical NOS. In case of unsuccessful completion, the trainee may seek reassessment on the Qualification Pack.

Method of assessment documentation and access

The assessment agency will upload the result of assessment in the portal. The data will not be accessible for change by the assessment agency after the upload. The assessment data will be validated by SSC assessment team. After upload, only SSC can access this data.

References

Glossary

Term	Description
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).
Training Outcome	Training outcome is a statement of what a learner will know, understand and be able to do **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.
National Occupational Standard	National Occupational Standard specify the standard of performance an individual must achieve when carrying out a function in the workplace
Performance Criteria	Performance Criteria indicates what specific characteristics an individual should be able to demonstrate in order to achieve the learning outcomes
Persons with Disability	Persons with Disability are those who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others.

Acronyms and Abbreviations

Term	Description
QP	Qualification Pack
NSQF	National Skills Qualification Framework
NSQC	National Skills Qualification Committee
NOS	National Occupational Standards
SSC	Skill Sectors Councils
NASSCOM	National Association of Software and Service Companies
NCO	National Classification of Occupations
ISCO	International Standard Classification of Occupations
ISIC	International Standard Industrial Classification
ISO	International Organization for Standardization
ICT	Information and Communication Technology
SLA	Service Level Agreement
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
OSI	Open Systems Interconnection
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TCP	Transmission Control Protocol
FTP	File Transfer Protocol
SSH	Secure Shell
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
VPN	Virtual Private Network
RDP	Remote Desktop Protocol
HTTPS	Hypertext Transfer Protocol Secure
2FA	Two-Factor Authentication
RDBMS	Relational Database Management System
SDLC	Software Development Lifecycle
CRM	Customer Relationship Management
PC	Performance Criteria
PwD	Persons with Disability