Model Curriculum

QF Name: Information Security Specialist

QF Code: SSC/Q0923

QF Version: 3.0

NSQF Level: 6

Model Curriculum Version: 3.0

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	Future Skills
Occupation	Cyber Security
Country	India
NSQF Level	6
Aligned to NCO/ISCO/ISIC Code	
Minimum Educational Qualification and Experience	* Relevant Field- Cybersecurity, Computer Science, IT **The relevant experience would include work, internship and apprenticeship undertaken post completion of relevant educational qualification Pursuing first year of 2-year PG program after completing 3 year UG degree OR Completed 4-year UG (in case of 4-year UG with honours/ honours with research) OR NSQF Level 5 STT with 3 years of relevant experience** in relevant field*
Pre-Requisite License or Training (Suggested but not mandatory)	NA
Minimum Job Entry Age	22 years
Last Reviewed On	03rd May 2023
Next Review Date	03rd May 2026
NSQC Approval Date	03rd May 2023
QF Version	3.0
Model Curriculum Creation Date	03rd May 2023
Model Curriculum Valid Up to Date	03rd May 2026
Model Curriculum Version	3.0

Minimum Duration of the Course	**600 hours**
Maximum Duration of the Course	**600 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.
- Describe the key security infrastructure components.
- Describe the methods of identifying and managing vulnerabilities in networks and devices.
- Implement security measures to protect data.
- Describe the strategies to evaluate security posture of an organization.
- Describe the methods to identify security risks using vulnerability assessment and penetration testing.
- Describe commonly employed cybersecurity measures in an organization
- Explain ways to manage vulnerabilities.
- Discuss key roles, departments and their functions commonly observed in an organization.
- Discuss correlations among the operations of various teams and operational best practices commonly observed in an organization.
- Describe the principles and techniques of project management.
- 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 QF.

NOS and Module Details	Theory Duration (In Hours)	Practical Duration (In Hours)	On-the-Job Training Duration (Mandatory)	On-the-Job Training Duration (Recommended)	Total Duration (In Hours)
Module 1 (Bridge Module): Information/Cyber Security – An Introduction	10:00	20:00	00:00	00:00	30:00
Module 2 (Bridge Module): Fundamental Concepts in Cyber Security	10:00	20:00	00:00	00:00	30:00
SSC/N0937 – Configure cybersecurity infrastructure components **NOS Version No. 2** **NSQF Level 6**	**20:00**	**40:00**	**00:00**	**00:00**	**60:00**
Module 3: Fundamentals of IT Security Infrastructure	20:00	40:00	00:00	00:00	60:00
SSC/N0938 – Maintain and enhance cybersecurity infrastructure	**20:00**	**40:00**	**00:00**	**00:00**	**60:00**

components **NOS Version No. 2** **NSQF Level 6**					
Module 4: Fundamentals of Security Infrastructure Components	10:00	20:00	00:00	00:00	30:00
Module 5: Security Mechanisms	10:00	20:00	00:00	00:00	30:00
SSC/N0939 – Define the cybersecurity infrastructure policy or technical security policy for an organization **NOS Version No. 2** **NSQF Level 6**	**30:00**	**60:00**	**00:00**	**00:00**	**90:00**
Module 6: Evaluating Organizational Security Posture using various Strategies	15:00	30:00	00:00	00:00	45:00
Module 7: Vulnerability Assessment and Penetration Testing	15:00	30:00	00:00	00:00	45:00
SSC/N0933 – Monitor and report on performance of operational and technical cybersecurity measures **NOS Version No. 2** **NSQF Level 6**	**20:00**	**40:00**	**00:00**	**00:00**	**60:00**
Module 8: Fundamentals of Cyber Security Measures	10:00	20:00	00:00	00:00	30:00
Module 9: Vulnerability Management and Legal Compliance	10:00	20:00	00:00	00:00	30:00
SSC/N0927 – Drive interrelated cybersecurity actions **NOS Version No. 2** **NSQF Level 6**	**10:00**	**20:00**	**00:00**	**00:00**	**30:00**
Module 10: Organizational Structure	05:00	10:00	00:00	00:00	15:00
Module 11: Interaction of Cyber Security with other Functions	05:00	10:00	00:00	00:00	15:00
SSC/N0928 – Manage a project team **NOS Version No. 2** **NSQF Level 6**	**10:00**	**20:00**	**00:00**	**00:00**	**30:00**
Module 12: Project Management	10:00	20:00	00:00	00:00	30:00
SSC/N9014 – Maintain an inclusive, environmentally sustainable workplace **NOS Version No. 1** **NSQF Level 5**	**10:00**	**20:00**	**0:00**	**0:00**	**30:00**

Module 13: Inclusive and environmentally sustainable workplaces	10:00	20:00	00:00	00:00	30:00
DGT/VSQ/N0102 **Employability Skill 60 Hours** **NOS Version No. 1** **NSQF Level 4**	**24:00**	**36:00**	**00:00**	**00:00**	**60:00**
Module 14: Introduction to Employability Skills	00:30	01:00	00:00	00:00	01.50
Module 15: Constitutional values - Citizenship	00:30	01:00	00:00	00:00	01.50
Module 16: Becoming a Professional in the 21st Century	01:00	01:30	00:00	00:00	02:50
Module 17: Basic English Skills	04:00	06:00	00:00	00:00	10:00
Module 18: Career Development & Goal Setting	01:00	01:00	00:00	00:00	02:00
Module 19: Communication Skills	02:00	03:00	00:00	00:00	05:00
Module 20: Diversity & Inclusion	01:00	01:30	00:00	00:00	02.50
Module 21: Financial and Legal Literacy	02:00	03:00	00:00	00:00	05:00
Module 22: Essential Digital Skills	04:00	06:00	00:00	00:00	10:00
Module 23: Entrepreneurship	03:00	04:00	00:00	00:00	07:00
Module 24: Customer Service	02:00	03:00	00:00	00:00	05:00
Module 25: Getting ready for apprenticeship & Jobs	03:00	05:00	00:00	00:00	08:00
OJT	00:00	00:00	120:00	0:00	120:00
Total Duration	**164:00**	**316:00**	**120:00**	**00:00**	**600:00**

Module Details

Module 1 Information/Cyber Security- An Introduction

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

<table>
<tr><td><b>Duration (In Hours)</b>: <i>05:00</i></td><td><b>Duration (In Hours)</b>: <i>04:00</i></td></tr>
<tr><td><b>Theory – Key Learning Outcomes</b></td><td><b>Practical – Key Learning Outcomes</b></td></tr>
<tr><td>• Explain the relevance of cybersecurity 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., IT Security Infrastructure Specialist)
• 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.</td><td>• Create a career map for roles in information/cybersecurity
• Demonstrate the working mechanism of malicious codes such as virus, malware, logic bomb, ransomware, spyware, phishing, trojan etc.</td></tr>
<tr><td colspan="2"><b>Classroom Aids:</b></td></tr>
<tr><td colspan="2">Whiteboard and markers
Chart paper and sketch pens
LCD Projector and Laptop for presentations</td></tr>
<tr><td colspan="2"><b>Tools, Equipment and Other Requirements</b></td></tr>
<tr><td colspan="2">Labs equipped with the following:
• PCs/Laptops
• Internet with Wi-Fi (Min. 2 Mbps dedicated)
• Samples of the templates and checklists used in organizations</td></tr>
</table>

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 (In Hours): *07:00*	**Duration (In Hours)**: *04:00*
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: Fundamentals of IT Security Infrastructure

Mapped to SSC/N0937 (Version 2)

Terminal Outcomes:

- Describe the key security infrastructure components and their protection mechanisms
- Evaluate the existing security posture of an organization and recommend suitable solutions

Duration (In Hours): *20:00*	**Duration (In Hours)**: *40:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Discuss the importance of security infrastructure in an organization. • Explain the key components of IT security infrastructure. • Describe and contrast various security protocols based on their features and functionalities. • Describe the parameters to monitor the functioning of infrastructure components. • Explain the protection mechanisms applied in securing an organization's infrastructure, including end-user devices. • Describe the types of firewall filtering technologies and methods to block unauthorized external devices (e.g., DVD, USB, etc.) • Discuss the importance of stakeholders to gather, validate and provide information related to information security incidents. • Discuss some examples of security incidents along with the methods to resolve them. • Explain the methods of password protection in configuration files.	• Demonstrate the configuration and testing of security infrastructure components. • Demonstrate the use of automated configuration tools in implementing baseline configurations. • Demonstrate the processes involved in implementing security protocols. • Demonstrate simulations to identify existing security protocols and security breaches. • Demonstrate the analysis of a sample network's current internet address range. • Demonstrate the management of unused interfaces of simulated network infrastructure. • Demonstrate the installation of firewalls. • Perform optimization of sample networks. • Demonstrate network access control (including permissions for protocols, ports, and IP addresses). • Demonstrate the blocking of unauthorized external devices. • Demonstrate the process of updating security infrastructure components and firewall settings.

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 4: Fundamentals of Security Infrastructure Components

Mapped to SSC/N0938 (Version 2)

Terminal Outcomes:

- Describe the methods of identifying and managing vulnerabilities in networks and devices

Duration (In Hours): *10:00*	**Duration (In Hours)**: *20:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Discuss the importance of identifying business functions, key cybersecurity activities, and corresponding stakeholders in managing network vulnerabilities • Describe Common Vulnerabilities and Exposures (CVE), and vulnerability detection methods • Discuss vulnerability scanning and common tools used for the same • Discuss various types of exploits such as worm, DoS, backdoor, etc. • Discuss penetration testing methods such as scanning, buffer overflow attacks, SQL injection, XSS, cookie theft, etc. to expose vulnerabilities in systems, servers, and applications • Explain the difference between vulnerability assessment and penetration testing • Describe various aspects of vulnerability management cycle • Describe the usage of logs in vulnerability management • Explain the concepts related to configuration management and patch management • Describe the sources to find vulnerability and patch information such as CERT	• Demonstrate the deployment of exploit frameworks • Carry out vulnerability assessments and integrity check of security systems using automated tools • Demonstrate the techniques of penetration testing such as reconnaissance, static and dynamic analysis, XSS, SQL injection, etc. • Demonstrate the process to determine vulnerability frequency and calculate vulnerability severity • Develop sample workflows for incident response management • Demonstrate the use of OVAL standards in vulnerability assessment • Demonstrate the process to interpret log summaries to identify anomalies • Demonstrate configuration and patch management • Demonstrate the preparation of reports on VAPT analysis
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 Tools and Programming Languages: • Security Methodologies and Vulnerability Frameworks like OWASP Top 10, PTES, MITRE ATT&CK etc.	

- IT Controls & Frameworks like SOX, ISO2700X, SANS, SOC2, CIS, COBIT, NIST etc.
- Awareness of Security Architecture frameworks like Defense-in-Depth Architecture, Micro-segmentation, Perimeter Security, Remote Access etc.
- Awareness of Security Modelling techniques like Zero-Trust Model, SASE Model etc.
- Vulnerability Scanning tools like Qualys, Burp Suite, Tenable Nessus, Netsparker etc.
- Penetration Testing tools like DirBuster, Nikto, Hydra, SQLMap, Netsparker, Burp Suite, etc.
- SIEM tools like ArcSight, QRadar, RSA NetWitness Suite, Splunk, LogRythym etc.
- Operating Systems like Kali Linux, Parrot OS, Windows, MacOS etc.
- Awareness of Virtualization techniques and Container services like Docker, Kubernetes, Amazon ECS etc.
- Cloud Environments like AWS, GCP, MS Azure etc.
- Monitoring tools such as Prometheus, Nagios, Icinga, etc.

Module 5: Security Mechanisms

Mapped to SSC/N0938 (Version 2)

Terminal Outcomes:

- Implement security measures to protect data.

Duration (In Hours): *10:00*	**Duration (In Hours):** *20:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• List the devices to be investigated. • Describe the scope and limitations for various security tools. • Explain the tools and techniques used in identifying and fixing data leaks. • Explain the working mechanism of proxy servers. • Explain the methods to perform functional and connectivity testing • Discuss the importance of maintaining server and other hardware • Describe commonly encountered issues in security component maintenance as well as the methods to resolve them • Discuss the tools used in TCP traffic analysis, detection of missing security patches, and security components testing • Discuss the importance of tracking OEMs and their solutions • Discuss the importance of various stakeholders in implementing security mechanisms.	• Demonstrate the functioning of various security mechanisms implemented in organizations such as firewalls, data leak prevention techniques, anti-malware, anti-virus, filtering rules to prevent unauthorized access, etc. • Demonstrate the installation and configuration of relevant security tools. • Demonstrate analysis of TCP traffic data • Demonstrate functional and connectivity testing of security components • Demonstrate repairs or upgrades on simulated security infrastructure components • Demonstrate troubleshooting of simulated security infrastructure components • Demonstrate the installation of server updates • Demonstrate the maintenance of server configurations • Demonstrate the patching of network vulnerabilities

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 case studies, templates and checklists used in organizations

Tools and Programming Languages:

- Security Methodologies and Vulnerability Frameworks like OWASP Top 10, PTES, MITRE ATT&CK etc.
- IT Controls & Frameworks like SOX, ISO2700X, SANS, SOC2, CIS, COBIT, NIST etc.
- Awareness of Security Architecture frameworks like Defense-in-Depth Architecture, Micro-segmentation, Perimeter Security, Remote Access etc.
- Awareness of Security Modelling techniques like Zero-Trust Model, SASE Model etc.
- SIEM tools like ArcSight, QRadar, RSA NetWitness Suite, Splunk, LogRythym etc.
- Monitoring tools such as Prometheus, Nagios, Icinga, etc.
- Log Analysis tools such as Nagios, ELK Stack, Graylog, etc.
- Traffic Analysis tools such as Wireshark, Nagios Core, NetXMS, etc.
- Malware Analysis tools such as OllyDbg, Volatility, etc.
- Awareness of Virtualization techniques and Container services like Docker, Kubernetes, Amazon ECS etc.
- Cloud Environments like AWS, GCP, MS Azure etc.
- Operating Systems like Kali Linux, Parrot OS, Windows, CentOS, Red Hat etc.

Module 6: Evaluating Organizational Security Posture using various Strategies

Mapped to SSC/N0939 (Version 2)

Terminal Outcomes:

- Describe the process of formulating and implementing cybersecurity policies in an organization.
- Describe the strategies to evaluate security posture of an organization.

Duration (In Hours): *15:00*	**Duration (In Hours):** *30:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe the legal and regulatory compliance standards relevant to cybersecurity that are commonly implemented by an organization. • Discuss common procedures, guidelines, and checklists used in maintaining security policies and standards. • Explain the difference between internal and external audit. • Discuss the importance of various stakeholders in evaluating an organization's security posture.	• Demonstrate the process of cybersecurity policy formulation and its implementation in an IT organization. • Demonstrate the workflows involved in documenting sample organizational policies and legislation standards. • Demonstrate the process of evaluating the policies and standards of a sample organization. • Perform internal and external audit to find anomalies and verify security posture of in sample organizations.

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

Tools and Programming Languages:

- Security Methodologies and Vulnerability Frameworks like OWASP Top 10, PTES, MITRE ATT&CK etc.
- IT Controls & Frameworks like SOX, ISO2700X, SANS, SOC2, CIS, COBIT, NIST etc.
- Monitoring tools such as Prometheus, Nagios, Icinga, etc.

Module 7: Vulnerability Assessment and Penetration Testing

Mapped to SSC/N0939 (Version 2)

Terminal Outcomes:

- Describe the methods to identify security risks using vulnerability assessment and penetration testing.

Duration (In Hours): *15:00*	**Duration (In Hours):** *30:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe the concepts of vulnerability assessment, threat modeling and penetration testing. • Evaluate a sample organization's network environment and identify security gaps. • Explain risk and risk management cycle in the context of IT security • Discuss the importance of risk appetite and acceptable risk levels for business requirements in determining risk management policies • Describe the processes involved in risk assessment and risk mitigation • Discuss commonly used risk management frameworks and methodologies • Describe commonly used defence mechanisms at different layers of security infrastructure • Describe the methods to evaluate existing security controls • Discuss possible anomalies in security, legal and regulatory compliance of the IT set-up of a sample organization • Explain the importance of documenting and sharing risk assessment results at the organizational level.	• Perform vulnerability assessment and penetration testing of sample systems using suitable tools. • Prepare a record of the process and results of vulnerability assessment and penetration testing. • Demonstrate continuous monitoring procedures. • Demonstrate the process of evaluating security controls. • Demonstrate security authorization and other risk assessment procedures. • Evaluate exposure to typical cyber threats using vulnerability assessment tools. • Demonstrate the use of risk management tools and frameworks and formulate risk mitigation 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 the case studies, templates and checklists used in organizations Tools and Programming Languages:	

- Security Methodologies and Vulnerability Frameworks like OWASP Top 10, PTES, MITRE ATT&CK etc.
- IT Controls & Frameworks like SOX, ISO2700X, SANS, SOC2, CIS, COBIT, NIST etc.
- Vulnerability Scanning tools like Qualys, Burp Suite, Tenable Nessus, Netsparker etc.
- Penetration Testing tools like DirBuster, Nikto, Hydra, SQLMap, Netsparker, Burp Suite, etc.
- Monitoring tools such as Prometheus, Nagios, Icinga, etc.
- Malware Analysis tools such as OllyDbg, Volatility, etc.
- Traffic Analysis tools such as Wireshark, Nagios Core, NetXMS, etc.
- Operating Systems like Kali Linux, Parrot OS, Windows, MacOS etc.
- Awareness of Virtualization techniques and Container services like Docker, Kubernetes, Amazon ECS etc.
- Cloud Environments like AWS, GCP, MS Azure etc.

Module 8: Fundamentals of Cyber Security Measures

Mapped to SSC/N0933 (Version 2)

Terminal Outcomes:

- Describe commonly employed cybersecurity measures in an organization

Duration (In Hours): *10:00*	**Duration (In Hours)**: *20:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Discuss the list of IT infrastructure components that must be investigated to ensure an organization's information security • Explain the common tools, methods, and KPIs used in infrastructure security monitoring, and routine maintenance of components • Discuss the frameworks, KPIs, and standards commonly employed in IT organizations for infrastructure security • Explain the techniques and countermeasures commonly employed in infrastructure security, including the use of proxy server and virus signature • Discuss open source and propriety anti-virus software available in the market for better security of end-user systems • Discuss the sources of information regarding security enhancement procedures	• Demonstrate the use of automated tools to implement and monitor cybersecurity measures • Perform an analysis of sample audit reports, risk assessment reports, and SIEM tool reports to: - monitor traffic trends - detect vulnerabilities as well as incidents of unauthorized access - assess the existing security posture - measure KPIs • Demonstrate the use of prescribed tools/software for documenting and updating security reports
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 Tools and Programming Languages: • Security Methodologies and Vulnerability Frameworks like OWASP Top 10, PTES, MITRE ATT&CK etc. • IT Controls & Frameworks like SOX, ISO2700X, SANS, SOC2, CIS, COBIT, NIST etc. • Cloud Environments like AWS, GCP, MS Azure etc. • Operating Systems like Kali Linux, Parrot OS, Windows, MacOS etc.	

Module 9: Vulnerability Management and Legal Compliance

Mapped to SSC/N0933 (Version 2)

Terminal Outcomes:

- Explain ways to manage vulnerabilities.

Duration (In Hours): *10:00*	Duration (In Hours): *20:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe the procedure to conduct vulnerability assessment. • Describe the processes for incident response management and prioritize vulnerabilities accordingly. • Explain the use of logs in identifying vulnerabilities. • Check log summaries to identify security issues. • Discuss the importance of various stakeholders in vulnerability management and legal compliance. • Discuss the regulations applicable to vulnerability management.	• Perform vulnerability assessment in sample system. • Prepare reports on vulnerability assessments. • Develop a methodology for log monitoring. • Perform system integrity check in sample systems. • Prepare a report on security performance parameters using suitable tools.
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 Tools and Programming Languages: • IT Controls & Frameworks like SOX, ISO2700X, SANS, SOC2, CIS, COBIT, NIST etc. • Vulnerability Scanning tools like Qualys, Burp Suite, Tenable Nessus, Netsparker etc. • Monitoring tools such as Prometheus, Nagios, Icinga, etc. • Log analysis tools such as Nagios, ELK Stack, Graylog, etc. • Awareness of Virtualization techniques and Container services like Docker, Kubernetes, Amazon ECS etc. • Cloud Environments like AWS, GCP, MS Azure etc. • Operating Systems like Kali Linux, Parrot OS, Windows, CentOS, Red Hat etc.	

Module 10: Organizational Structure

Mapped to SSC/N0927 (Version 2)

Terminal Outcomes:

- Discuss key roles, departments and their functions commonly observed in an organization.

<table>
<tr><td><b>Duration (In Hours):</b> <i>05:00</i></td><td><b>Duration (In Hours):</b> <i>10:00</i></td></tr>
<tr><td><b>Theory – Key Learning Outcomes</b></td><td><b>Practical – Key Learning Outcomes</b></td></tr>
<tr><td>• Describe various business functions commonly found in organizations based on their industry and size.
• Explain the roles, responsibilities, interests, and concerns of the stakeholders in various business functions, including cybersecurity.
• Evaluate the relevance of various teams and stakeholders for the business objectives of a firm.</td><td>• Demonstrate sample organization structures and identify in them:
– key business functions, key stakeholders, and their responsibilities.
– business functions that have a joint working relationship with the cyber security function.</td></tr>
<tr><td colspan="2"><b>Classroom Aids:</b></td></tr>
<tr><td colspan="2">Whiteboard and markers
Chart paper and sketch pens
LCD Projector and Laptop for presentations</td></tr>
<tr><td colspan="2"><b>Tools, Equipment and Other Requirements</b></td></tr>
<tr><td colspan="2">Labs equipped with the following:
• PCs/Laptops
• Internet with Wi-Fi (Min. 2 Mbps dedicated)
• Samples of the case studies, templates and checklists used in organizations</td></tr>
</table>

Module 11: Interaction of Cyber Security with other Functions

Mapped to SSC/N0927 (Version 2)

Terminal Outcomes:

- Discuss correlations among the operations of various teams and operational best practices commonly observed in an organization.

Duration (In Hours): *05:00*	**Duration (In Hours):** *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe best practices pertaining to the interaction of cybersecurity teams (related to business functions, and security operations) with other teams and key stakeholders. • Describe the importance of stakeholder management in the context of security operations. • Explain the dependency management best practices adopted by organizations to coordinate cross-functional activities related to cybersecurity. • Describe the operating procedures that are applicable to the systems being used, typical response times and service times. • List organizational systems, procedures and tasks/ checklists related to cybersecurity in sample organizations.	• Prepare an inventory of roles that are responsible or accountable for cyber security activities, functions, and operations in sample organizations. • Prepare an inventory of operations that fall into various key cyber security activities in sample organizations. • Demonstrate sample workflows pertaining to the distribution of cybersecurity responsibilities. • Apply the principles of stakeholder management for effective communication, conflict resolution, fulfilment of agreements and continuous improvement.

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 case studies, templates and checklists used in organizations

Module 12: Project management

Mapped to SSC/N0928 (Version 2)

Terminal Outcomes:

- Describe the principles and techniques of project management.

Duration (In Hours): *10:00*	**Duration (In Hours)**: *20:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the fundamentals of project life cycle, agile project management, and organization structure for projects • Discuss the importance of project scope, and scheduling of activities for effective resource management. • Explain commonly used resource estimation procedures. • Explain the process of work allocation in line with project objectives. • Explain the concept of continuous evaluation in relation to project management and team performance. • Discuss the functions and staffing needs of the audit team. • Describe the steps involved in project auditing. • Evaluate performance indicators of the project as well as team members in a sample project.	• Demonstrate the process of defining project scope and preparing a project plan for a sample project. • Demonstrate the process of scheduling activities and resource management. • Apply the principles of effective team management such as team building, team motivation, conflict resolution and constructive feedback. • Perform a simulation of sample project evaluation, continuous review, and team coordination. • Perform a simulation of preparing and updating work plans.
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 case studies, templates and checklists used in organizations Tools and Programming Languages: • Workflow Management tools such as JIRA, Kanboard, Wekan, etc.	

Module 13: 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 (In Hours): *10:00*	**Duration (In Hours)**: *20:00*
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)	

Module 14: Introduction to Employability Skills

Mapped to NOS DGT/VSQ/N0102 (Version No. 1)

Key Learning Outcomes:

- Discuss the Employability Skills required for jobs in various industries
- List different learning and employability related GOI and private portals and their usage

Duration:1.5 Hours (0.5 Theory + 1 Practical)

Module 15: Constitutional values - Citizenship

Mapped to NOS DGT/VSQ/N0102 (Version 1)

Key Learning Outcomes:

- Explain the constitutional values, including civic rights and duties, citizenship, responsibility towards society and personal values and ethics such as honesty, integrity, caring and respecting others that are required to become a responsible citizen
- Show how to practice different environmentally sustainable practices

Duration:1.5 Hours (0.5 Theory + 1 Practical)

Module 16: Becoming a Professional in the 21st Century

Mapped to NOS DGT/VSQ/N0102 (Version 1)

Key Learning Outcomes:

- Discuss importance of relevant 21st century skills.
- Exhibit 21st century skills like Self-Awareness, Behaviour Skills, time management, critical and adaptive thinking, problem-solving, creative thinking, social and cultural awareness, emotional awareness, learning to learn etc. in personal or professional life.
- Describe the benefits of continuous learning

Duration:2.5 Hours (1 Theory + 1.5 Practical)

Module 17: Basic English Skills

Mapped to NOS DGT/VSQ/N0102 (Version 1)

Key Learning Outcomes:

- Show how to use basic English sentences for everyday conversation in different contexts, in person and over the telephone
- Read and interpret text written in basic English
- Write a short note/paragraph / letter/e -mail using basic English

Duration: 10 Hours (4 Theory + 6 Practical)

Module 18: Career Development and Goal Setting

Mapped to NOS DGT/VSQ/N0102 (Version 1)

Key Learning Outcomes:

- Create a career development plan with well-defined short- and long-term goals

Duration: 2 Hours (1 Theory + 1 Practical)

Module 19: Communication skills

Mapped to NOS DGT/VSQ/N0102 (Version 1)

Key Learning Outcomes:

- Demonstrate how to communicate effectively using verbal and nonverbal communication etiquette.
- Explain the importance of active listening for effective communication
- Discuss the significance of working collaboratively with others in a team

Duration: 5 Hours (2 Theory + 3 Practical)

Module 20: Diversity & Inclusion

Mapped to NOS DGT/VSQ/N0102 (Version 1)

Key Learning Outcomes:

- Demonstrate how to communicate effectively using verbal and nonverbal communication etiquette.
- Explain the importance of active listening for effective communication
- Discuss the significance of working collaboratively with others in a team

Duration: 2.5 Hours (1 Theory+ 1.5 Practical)

Module 21: Financial and Digital Literacy

Mapped to NOS DGT/VSQ/N0102 (Version 1)

Key Learning Outcomes:

- Outline the importance of selecting the right financial institution, product, and service
- Demonstrate how to carry out offline and online financial transactions, safely and securely

Duration: 5 Hours (2 Theory+ 3 Practical)

Module 22: Essential Digital Skills

Mapped to NOS DGT/VSQ/N0102 (Version 1)

Key Learning Outcomes:

- Describe the role of digital technology in today's life
- Demonstrate how to operate digital devices and use the associated applications and features, safely and securely
- Discuss the significance of displaying responsible online behaviour while browsing, using various social media platforms, e-mails, etc., safely and securely
- Create sample word documents, excel sheets and presentations using basic features
- utilize virtual collaboration tools to work effectively

Duration: 10 Hours (4 Theory+ 6 Practical)

Module 23: Entrepreneurship

Mapped to NOS DGT/VSQ/N0102 (Version 1)

Key Learning Outcomes:

- Explain the types of entrepreneurship and enterprises
- Discuss how to identify opportunities for potential business, sources of funding and associated financial and legal risks with its mitigation plan
- Describe the 4Ps of Marketing-Product, Price, Place and Promotion and apply them as per requirement
- Create a sample business plan, for the selected business opportunity

Duration: 7 Hours (3 Theory+ 4 Practical)

Module 24: Customer Service

Mapped to NOS DGT/VSQ/N0102 (Version 1)

Key Learning Outcomes:

- Describe the significance of analysing different types and needs of customers
- Explain the significance of identifying customer needs and responding to them in a professional manner.
- Discuss the significance of maintaining hygiene and dressing appropriately

Duration: 5 Hours (2 Theory+ 3 Practical)

Module 25: Getting Ready for Apprenticeship and Jobs

Mapped to NOS DGT/VSQ/N0102 (Version 1)

Key Learning Outcomes:

- Create a professional Curriculum Vitae (CV)
- Use various offline and online job search sources such as employment exchanges, recruitment agencies, and job portals respectively
- Discuss the significance of maintaining hygiene and confidence during an interview
- Perform a mock interview
- List the steps for searching and registering for apprenticeship opportunities

Duration: 8 Hours (3 Theory+ 5 Practical)

Annexure

Trainer Requirements

Trainer Prerequisites						
Minimum Educational Qualification	**Specialization**	**Relevant Industry Experience**		**Training Experience**		**Remarks**
		Years	***Specialization***	***Years***	***Specialization***	
Graduate	Engineering/ Technology/ Statistics/ Mathematics/ Computer Science	2 years of full-time work experience in IT Security Infrastructure Specialist or relevant roles	The full-time experience would include work, internship and apprenticeship undertaken post completion of regular graduation	1 year of full-time work experience in IT Security Infrastructure Specialist or relevant roles		

Trainer Certification	
Domain Certification	**Platform Certification**
Certified for Job Role: "IT Security Infrastructure Specialist" mapped to QF: "SSC/Q0923, V2.0". Minimum accepted score is 80%	Recommended that the trainer is certified for the Job role "Trainer" mapped to the Qualification File "MEP/Q2601, V1.0". Minimum accepted score is 80% aggregate

Assessor Requirements

<table>
<tr><th colspan="7">Assessor Prerequisites</th></tr>
<tr><th rowspan="2">Minimum Educational Qualification</th><th rowspan="2">Specialization</th><th colspan="2">Relevant Industry Experience</th><th colspan="2">Training Experience</th><th rowspan="2">Remarks</th></tr>
<tr><th><i>Years</i></th><th><i>Specialization</i></th><th><i>Years</i></th><th><i>Specialization</i></th></tr>
<tr><td>Graduate</td><td>Engineering/ Technology/ Statistics/ Mathematics/ Computer Science</td><td>2 years of full-time work experience in IT Security Infrastructure Specialist or relevant roles</td><td>The full-time experience would include work, internship and apprenticeship undertaken post completion of regular graduation</td><td>1 year of full-time work experience in IT Security Infrastructure Specialist or relevant roles</td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="2">Assessor Certification</th></tr>
<tr><th>Domain Certification</th><th>Platform Certification</th></tr>
<tr><td>Certified for Job Role: “IT Security Infrastructure Specialist” mapped to QF: “SSC/Q0923, V2.0”. Minimum accepted score is 80%</td><td>Recommended that the trainer is certified for the Job role “Assessor” mapped to the Qualification File “MEP/Q2701, V1.0”. Minimum accepted score is 80% aggregate</td></tr>
</table>

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 File 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 QF, a trainee should score an average of 70% or more . In case of unsuccessful completion, the trainee may seek reassessment on the Qualification File.

Method of assessment documentation and access

The assessment agency will upload the result of the 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.

Recommended Supplemental Readings

The learning modules covered in the Model Curriculum for IT Security Infrastructure Specialist are designed to meet the expected outcomes as per the QF. While the modules aligned to NOS are focused on technical/ behavioral competencies, bridge modules cover the prerequisite/ preparatory topics that are indispensable to complete the course. However, to provide additional QF specific knowledge to the learners, the following supplemental readings on related topics are recommended. These readings will equip the learners with an understanding of advanced or ancillary concepts to take up more complex tasks as listed in the QF.

QF	Recommended Supplemental Reading
SSC/Q0923: IT Security Infrastructure Specialist	1. Zero Trust Network Access 2. Data Privacy Safeguards 3. Cryptography 4. Security Orchestration Automation and Response (SOAR) 5. Managed Detection and Response

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
QF	Qualification File
NSQF	National Skills Qualification Framework
NSQC	National Skills Qualification Committee
NOS	National Occupational Standards
SSC	Skill Sectors Councils
NASSCOM	National Association of Software & Service Companies
NCO	National Classification of Occupations
ISCO	International Standard Classification of Occupations
ISIC	International Standard Industrial Classification
ISO	International Organization for Standardization
SLA	Service Level Agreement
ICT	Information and Communication Technology
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
MFA	Multi-Factor Authentication
XSS	Cross-site Scripting
VAPT	Vulnerability Assessment and Penetration Testing
CERT	Computer Emergency Response Team
OVAL	Open Vulnerability and Assessment Language
RDBMS	Relational Database Management System
SDLC	Software Development Lifecycle
OEM	Original Equipment Manufacturer
GRC	Governance, Risk management and Compliance
PwD	Persons with Disability
SIEM	Security Information and Event Management
CRM	Customer Relationship Management
PC	Performance Criteria