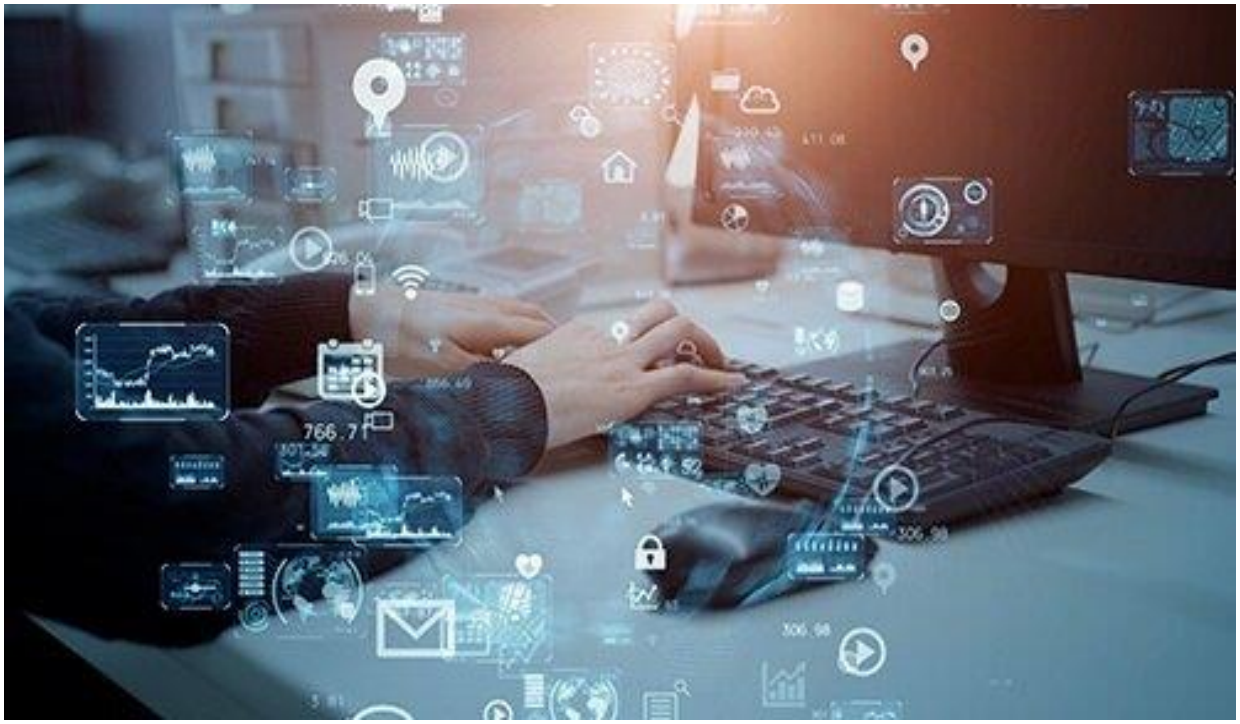

Model Curriculum

QF Name: Cybersecurity

QF Version: 1.0

NSQF Level: 4.5

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	**Future Skills**
Occupation	**Cyber Security**
Country	**India**
NSQF Level	**4.5**
Aligned to NCO/ISCO/ISIC Code	**NCO-2015/ NIL**
Minimum Educational Qualification and Experience	➢ Completed 1st year of 3-year/ 4-years UG OR ➢ Pursuing 1st year of 3-year/ 4-years UG and continuing education OR ➢ Previous relevant Qualification of NSQF Level 4 with 1.5 years of relevant experience
Pre-Requisite License or Training	**NA**
Minimum Job Entry Age	**19 years**
Last Reviewed On	**TBD**
Next Review Date	**TBD**
NSQC Approval Date	**TBD**
QF Version	**1.0**
Model Curriculum Creation Date	**TBD**
Model Curriculum Valid Up to Date	**TBD**
Model Curriculum Version	**1.0**
Minimum Duration of the Course	**510 hours**
Maximum Duration of the Course	**510 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.

- Demonstrate how to maintain a healthy, safe and secure environment at workplace.
- Illustrate sustainable practices at workplace for energy efficiency and waste management
- 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 typical vulnerabilities observed in applications.
- Describe the methods to identify vulnerabilities in applications.
- Demonstrate the ways to perform vulnerability assessment in applications.
- Evaluate implemented IdAM solutions to ensure adherence to architectural objectives
- Describe the policies, standards, procedures, and guidelines related to application security.
- Discuss the latest technological developments in application security.
- Perform vulnerability analysis using suitable tools.
- Demonstrate the extraction of relevant data or information from forensic evidence.
- Explain the functionalities of forensic analysis tools.
- Demonstrate methods to manage security risks and to conduct security audits
- Demonstrate different ways to enhance existing security solutions
- 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.

Compulsory Modules

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

NOS and Module Details	Theory Duration	Practical Duration (In Hours)	On-the-Job Training Duration (Mandatory)	On-the-Job Training Duration (Recommended)	Total Duration (In Hours)
SSC/N0943:Work organization and management for cyber security NSQF level :4.5 NOS Version 1	10:00	20:00	00:00	00:00	30:00
SSC/N0944:Communication and interpersonal skills for cyber security NSQF level :4.5 NOS Version 1	10:00	20:00	00:00	00:00	30:00
SSC/N0945 :Secure systems design and creation NSQF level :4.5 NOS Version 1	20:00	40:00	00:00	00:00	60:00

Module 1: Fundamentals of IT Security Infrastructure	20:00	40:00	00:00	00:00	60:00
SSC/N0946: Secure systems operation and maintenance NSQF level :4.5 NOS Version 1	**30:00**	**60:00**	**00:00**	**00:00**	**90:00**
Module 2: Network Security Fundamentals	05:00	10:00	00:00	00:00	15:00
Module 3: Fundamentals of Security Infrastructure Components	05:00	10:00	00:00	00:00	15:00
Module 4: Security Mechanisms	05:00	10:00	00:00	00:00	15:00
Module5: Analysis and Evaluation of the IdAM Solutions	05:00	10:00	00:00	00:00	15:00
Module 6: Identity management and Compliance Correlation	05:00	10:00	00:00	00:00	15:00
Module 7: Security Audit	05:00	10:00	00:00	00:00	15:00
SSC/N0947:Secure systems protection and defense NSQF level :4.5 NOS Version 1	**60:00**	**120:00**	**00:00**	**00:00**	**180:00**
Module 8: Application Vulnerabilities	10:00	20:00	00:00	00:00	30:00
Module 9: Identification of Vulnerabilities	10:00	20:00	00:00	00:00	30:00
Module 10: Threat/ Vulnerability Analysis	05:00	10:00	00:00	00:00	15:00
Module 11: Application Hardening	05:00	10:00	00:00	00:00	15:00
Module 12: Configuration Management	05:00	10:00	00:00	00:00	15:00
Module 13: Web Application Secure Configuration	05:00	10:00	00:00	00:00	15:00
Module 14: Patch Management	05:00	10:00	00:00	00:00	15:00
Module 15: Endpoint Security System Functionality	05:00	10:00	00:00	00:00	15:00
Module 16: Endpoint Security Measures	05:00	10:00	00:00	00:00	15:00
Module 17: Security Solutions for Endpoint Devices	05:00	10:00	00:00	00:00	15:00
SSC/N0948 :Operations and Management NSQF level :4.5 NOS Version 1 SSC/N0949 :Intelligence collection and analysis NSQF level :4.5 NOS Version 1	**20:00**	**40:00**	**00:00**	**00:00**	**60:00**
Module 18: Monitoring and data collection	10:00	20:00	00:00	00:00	30:00
Module 19: Basic Analysis	10:00	20:00	00:00	00:00	30:00

SSC/N0950 :Investigation and Digital Forensics NSQF level :4.5 NOS Version 1	**20:00**	**40:00**	**00:00**	**00:00**	**60:00**
Module 20: First Response to a Cyber Crime Incident	02:50	05:00	00:00	00:00	07:50
Module 21: Search and Seizure	02:50	05:00	00:00	00:00	07:50
Module 22: Cyber Security Policies, Procedures, Standards & Guidelines	02:50	05:00	00:00	00:00	07:50
Module 23: Data Acquisition from Storage Devices, Network Traffic and Operating Systems	02:50	05:00	00:00	00:00	07:50
Module 24: Cyber Forensic Analysis	05:00	10:00	00:00	00:00	15:00
Module 25: Analysis Tools	05:00	10:00	00:00	00:00	15:00
Total Duration	**170:00**	**340:00**	**00:00**	**00:00**	**510:00**

SSC/N0943: Work Organization and Management for cyber security

Duration: *10:00(In Hours)*	**Duration:** *20:00(In Hours)*
Key Learning Outcomes- Theory	**Key Learning Outcomes- Practical**
• Troubleshoot common web design and development problems. • Work within specified time limitations and deadlines • Use a computer with a range of software packages. • Apply research techniques and skills to keep up to date with industry best practices. • Apply deployment optimization, such as page loading, with industry best practices. • Ensure the work is completed according to a given schedule. • Include linked images, fonts, native files, and production file format when archiving. • Use software version control systems such as git.	• Demonstrate management skills in a work organization.
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) Microphone / voice system for lecture and class activities Computer Lab with 1:1 PC: trainee ratio and having internet connection, MS Office / Open office, Browser,Outlook / Any other Email Client, and chat tools	

SSC/N09444: Communication and interpersonal skills for cyber security

Duration: *10:00(In Hours)*	**Duration:** *20:00(In Hours)*
Key Learning Outcomes- Theory	**Key Learning Outcomes- Practical**
• Read and understand specifications documents • Read and use provided source code of front-end and back-end • technologies • Deliver products that respond to client requirements and • specification • Gather, analyse, and evaluate information • Interpret standards and requirements • Match client requirements • Present concepts to meet business requirements	Demonstrate communication skills to meet business requirements.
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) Microphone / voice system for lecture and class activities Computer Lab with 1:1 PC: trainee ratio and having internet connection, MS Office / Open office, Browser,Outlook / Any other Email Client, and chat tools

Module Details

Module 1: Fundamentals of IT Security Infrastructure

Mapped to SSC/N0945 (Version 1)

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 2: Network Security Fundamentals

Mapped to SSC/N0946 (Version 1)

Outcomes:

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

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
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. • Discuss the types of electronic evidence and networking concepts relevant to them. • List the devices containing electronic evidence in sample systems. • Describe the process of forensic investigation.	• 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 cyberattacks. • Demonstrate the analysis of sample ICT devices for evidence.
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 Security Infrastructure Components

Mapped to SSC/N0946 (Version 1)

Terminal Outcomes:

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

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
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 4: Security Mechanisms

Mapped to SSC/N0946 (Version 1)

Terminal Outcomes:

- Implement security measures to protect data.

Duration (In Hours): *5:00*	**Duration (In Hours)**: *10:00*
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 5: Analysis and Evaluation of the IdAM Solutions

Mapped to SSC/N0946 (Version 1)

Terminal Outcomes:

- Evaluate implemented IdAM solutions to ensure adherence to architectural objectives.

Duration: *5:00*	**Duration**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe steps involved in integrating IdAM solutions with existing login systems or SIEM software. • Describe the importance for IdAM solutions to be compliant with policies, standards, regulations, etc. • Describe the audit and reporting process to clarify how systems and information can be used. • Discuss the need to track user activities across systems and IdAM solutions. • Discuss the need to modify access controls in line with users changing responsibilities, including removal of access when no longer required. • Discuss guidelines for continuous monitoring processes that constantly close security gaps and improve business operations.	• Demonstrate functional testing of sample IdAM solutions to evaluate performance against architectural designs and requirements. • Demonstrate non-function testing of IdAM solutions to evaluate features such as usability, reliability, performance, etc. • Perform a comparative analysis of sample implemented solutions against the prescribed architectural design to ensure they satisfy architectural objectives and adhere to design. • Demonstrate how to modify access controls in line with users changing responsibilities, including removal of access when no longer required.
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) • IdAM technologies and protocols that include Active Directory, Directory Services, LDAP, MFA system, etc. • Samples of applications (computer, mobile and cloud applications) that require access rights Tools and Programming Languages: • IdAM tools such as Open IAM, Apache Syncope, WSO2 Identity, etc. • Markup Languages such as XML, SAML, etc. • Programming Languages: Java, PHP, Go, etc.	

Module 6: Identity management and Compliance Correlation

Mapped to SSC/N0946 (Version 1)

Terminal Outcomes:

- Evaluate implemented IdAM solutions to ensure adherence to compliance requirements.

Duration: *05:00*	**Duration**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe information security concepts, policies, and procedures. • Explain the methods and tools to assess if the implemented solution is satisfying compliance requirements. • Explain the methods and tools to monitor access controls in relation to regulatory compliance for sensitive data. • Discuss the importance of various stakeholders related to compliance requirements of IdAM solutions.	• Demonstrate how to assess if implementation is satisfying compliance requirements. • Demonstrate how to monitor access controls in relation to regulatory compliance for sensitive data.
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) • IdAM technologies and protocols that include Active Directory, Directory Services, LDAP, MFA system, etc. • Samples of applications (computer, mobile and cloud applications) that require access rights Tools and Programming Languages: • IdAM tools such as Open IAM, Apache Syncope, WSO2 Identity, etc. • Markup Languages such as XML, SAML, etc. • Programming Languages: Java, PHP, Go, etc.	

Module 7: Security Audit

Mapped to SSC/N0946 (Version 1)

Terminal Outcomes:

- Discuss how audit tasks are performed in various organizations

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the process of technical evaluation of various ICT components to ensure relevant Confidentiality, Integrity and Availability (CIA) compliances. • Describe the audit techniques used in internal, external and third-party audits. • Explain the importance of SLAs and other prescribed standards in compliance audit and analysis. • Discuss the templates and KPIs used to report compliance audit and analysis results.	• Demonstrate sample audit processes using prescribed methods and tools. • Perform configuration reviews of sample information security systems using automated tools. • Prepare a report for the sample audit, including scope, evidence, artefacts, procedure, guidelines, and results, using standards templates and 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: • Security Auditing tools such as Open Audit, Gensuite, etc. • Programming languages such as Python, C/C++, Java, Ruby, etc. • Operating Systems like Linux, Unix, Windows, CentOS, macOS, Red Hat etc.	

Module 8: Application Vulnerabilities

Mapped to SSC/N0947, v1.0

Terminal Outcomes:

- Describe typical vulnerabilities observed in applications.

Duration (In Hours): *10:00*	**Duration (In Hours)**: *20:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Define the types of vulnerabilities commonly found in applications. • Explain the procedure to identify application vulnerabilities.	• Demonstrate how to identify vulnerabilities in sample applications. • Demonstrate the functionalities of sample application and database layer IPS/IDS appliance.
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 Security Templates from ITIL • Samples of secure and unsecured applications of each category including various types of computer applications, mobile applications, and cloud applications, etc. • Access to public databases and vulnerability sharing clubs, e.g., Bugtraq, National Institute of Standards and Technology (NIST) National Vulnerability Database, United States Computer Emergency Readiness Team (US-CERT)	

Module 9: Identification of Vulnerabilities

Mapped to SSC/N0947, v1.0

Terminal Outcomes:

- Describe the methods to identify vulnerabilities in applications.

Duration (In Hours): *10:00*	**Duration (In Hours)**: *20:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the steps to gather relevant information for vulnerability assessment including: – source code – application type – security controls and application patching – application functionality and connectivity – application design and architecture • Discuss the importance of documentation review in identifying vulnerabilities. • Explain how to distinguish false positives form genuine security threats. • Explain the methods to identify application vulnerabilities. • Describe the methods and tools used in application penetration testing. • Explain the difference between internal and external penetration testing.	• Perform source code review using suitable methods and tools to identify security issues. • Demonstrate identification of potential threats by using threat scenarios from various sources. • Perform root cause analysis of identified issues in sample applications. • Demonstrate penetration testing processes and black box testing on sample applications using automatic scanning technologies and manual tests. • Perform network penetration testing by capturing a variety of traffic, poisoning of a victim's proxy server, hiding of sensitive information, hijacking of a variety of sessions etc. for building secure infrastructure. • Perform an external penetration test by creating topological network maps. • Demonstrate methods to document application security requirements. • Demonstrate methods to preserve data collected during the analysis.
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 Security Templates from ITIL • Samples of applications of each category including various types of computer applications, mobile applications, and cloud applications, etc.	

Tools and Programming Languages:

- Programming languages like PHP, Java, Python, or Go
- Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc.
- Application Security Testing (Static/Dynamic/Interactive) tools like IBM AppScan, HP Fortify, Burp Suite, Synopsys etc.
- Application Vulnerability Scanners like Grabber, Vega, Qualys, AppScan, etc.
- Code Scanner/Analysis tools such as OllyDbg, Agnitio, Checkmarx, Raxis, etc.
- Open-source Security tools like Nessus, Nmap, Metasploit Community edition, etc.
- Monitoring tools such as Prometheus, Nagios, Icinga, etc.

Module 10: Threat/ Vulnerability Analysis

Mapped to SSC/N0947, v1.0

Terminal Outcomes:

- Demonstrate the ways to perform vulnerability assessment in applications.

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain various vulnerability categories. • Describe ways to identify the extent of vulnerability in an application. • Describe the functionalities of commonly used vulnerability assessment tools and frameworks. • Discuss the best practices related to vulnerability assessment.	• Prepare a tracker in prescribed format to capture vulnerabilities and risk exposure data of sample applications. • Demonstrate categorization of vulnerabilities based on level of weakness, sensitivity of information, relevance, root causes, risk criticality, and mitigation methods. • Perform root cause analysis of identified vulnerabilities in sample applications. • Prepare a report on vulnerability analysis including security requirements, vulnerabilities identified and recommended solutions. • Demonstrate the procedure to securely store data collected during the assessment, vulnerabilities, analysis results, and mitigation recommendations.
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 Security Templates from ITIL • Samples of applications of each category including various types of computer applications, mobile applications, and cloud applications, etc. • Samples of secure and unsecured applications for practicing penetration testing activities Tools and Programming Languages: • Programming languages like PHP, Java, Python, or Go • Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc. • Application Security Testing (Static/Dynamic/Interactive) tools like IBM AppScan, HP Fortify, Burp Suite, Synopsys etc. • Application Vulnerability Scanners like Grabber, Vega, Qualys, AppScan, etc.	

- Code Scanner/Analysis tools such as OllyDbg, Agnitio, Checkmarx, Raxis, etc.
- Patch Management software like Solar Winds Patch Manager, ManageEnginer, etc.
- Open-source Security tools like Nessus, Nmap, Metasploit Community edition, etc.
- Log Analysis tools such as Nagios, ELK Stack, Graylog, etc.
- Monitoring tools such as Prometheus, Nagios, Icinga, etc.
- Documentation software such as MS-Word, Adobe, etc.

Module 11: Application Hardening

Mapped to SSC/N0947, v1.0

Terminal Outcomes:

- Describe the methods to perform application hardening.

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Discuss the steps involved in application hardening. • Explain the methods and tools to harden applications across devices and environments. • Discuss the best practices related to application hardening.	• Perform application hardening in sample applications.
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 secure and unsecured applications Tools and Programming Languages: • Programming Languages for Application Hardening: JavaScript, Perl, Python, Ruby, etc. • Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc.	

Module 12: Configuration Management

Mapped to SSC/N0947, v1.0

Terminal Outcomes:

- Describe the methods to secure application configuration across environments

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the methods and tools to securely configure applications. • Outline the importance of access controls in applications and databases. • Describe various security technical implementation guides (STIGs). • Discuss the best practices related to application configuration across environments.	• Demonstrate the process of securing administrative console using sample. web servers and applications • Demonstrate ways to manage unauthorized instances and extraneous functionalities. • Demonstrate the process of securing application configuration using tools and techniques such as application testing, code review, firewall, 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 secure and unsecured applications

Tools and Programming Languages:

- Programming Languages for Application Configuration: JavaScript, Perl, Python, Ruby, etc
- Application Security Testing (Static/Dynamic/Interactive) tools like IBM AppScan, HP Fortify, Burp Suite, Synopsys etc.
- Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc.
- Monitoring tools such as Prometheus, Nagios, Icinga, etc.

Module 13: Web Application Secure Configuration

Mapped to SSC/N0947, v1.0

Terminal Outcomes:

- Describe the methods to secure web application configurations.

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe the methods to configure web applications securely across environments for minimum exposure and weaknesses. • Discuss the best practices related to web application configuration.	• Demonstrate the process of securing web application configuration using tools and techniques such as application testing, code review, web application firewall, etc. • Apply suitable programming tools and techniques to configure, modify and debug application codes.
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 secure and unsecured applications Tools and Programming Languages: • Programming Languages for Application Configuration: JavaScript, Perl, Python, Ruby, etc • Application Security Testing (Static/Dynamic/Interactive) tools like IBM AppScan, HP Fortify, Burp Suite, Synopsys etc. • Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc. • Monitoring tools such as Prometheus, Nagios, Icinga, etc.	

Module 14: Patch Management

Mapped to SSC/N0947, v1.0

Terminal Outcomes:

- Define strategy for the management of patches and updates considering various relevant factors.
- Apply different approaches to manage web server, web application, and accessibility patches as per the latest guidelines.

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe patch management life cycle. • Define measures to effectively patch an application. • Outline the guidelines in relation to application patching and hardening. • Explain mechanisms to ensure implementation of security updates and patches on all application assets. • Describe the process of application hardening.	• Apply checks on front-end and back-end platforms for the reported vulnerabilities, and available patches or updates. • Demonstrate the implementation of latest or updated patches on all applications. • Demonstrate the integration of patch management with the operational cycle of IT infrastructure management. • Demonstrate the process of application hardening to reduce vulnerability. • Develop a strategy for management of patches and updates. • Demonstrate how to align or reengineer IT infrastructure processes as per the applications' patch management requirements.
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 secure and unsecured applications Tools and Programming Languages: • Programming languages like JavaScript, Perl, PHP, Python, Ruby, etc. • Patch Management software like Solar Winds Patch Manager, ManageEnginer, etc. • Code Scanner/Analysis tools such as OllyDbg, Agnitio, Checkmarx, Raxis, etc. • Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc.	

Module 15: Endpoint Security System Functionality

Mapped to SSC/N0947, v1.0

Terminal Outcomes:

- Explain the functionality of endpoint security platforms.
- Recommend security solutions by analyzing the maturity of endpoint security in existing systems.

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the working mechanism of an endpoint security platform. • Examine a sample organization's knowledge base for information on previous security incidents and how they were managed. • Explain the difference in traditional and continuous endpoint security compliance models for building a robust security posture.	• Carry out procedures for threat detection and mitigation as per their occurrences in sample endpoint systems. • Demonstrate how to record, classify, and prioritize the security events to be analyzed through BYOD. • Demonstrate methods to analyze 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: • Vulnerability Scanning tools like Qualys, Burp Suite, Netsparker, SQLMap, OpenVAS etc. • Source code analysis tools such as Code sonar, Coverity, HCL Appscan, etc. • Programming Languages for such as C++, Java, Python, Go, etc. • End-point security software such as EnCase, Tripwire, McAffee, etc. • EDR tools like SentinelOne, CrowdSec, VMware Carbon Black EDR, FireEye EDR etc. • Cloud Environments like AWS, GCP, MS Azure etc. • Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc.	

Module 16: Endpoint Security Measures

Mapped to SSC/N0947, v1.0

Terminal Outcomes:

- Explain popular measures to monitor endpoint protection.
- Explain how to configure and upgrade endpoint security management tools.

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• List the endpoint devices to be installed, configured, and troubleshoot. • 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. • Outline the best practices and general instructions/ guidelines related to installation and configuration of endpoint devices. • Outline the best practices and general instructions/ guidelines related to resolution of security issues in endpoint devices.	• Demonstrate how to install and configure endpoint devices as per prescribed guidelines. • 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 security monitoring and troubleshooting tools. • Demonstrate the configuration and upgradation of endpoint security environment and clients. • Demonstrate ways to optimize the deployment manager. • Prepare reports on troubleshooting, configurations, and deployment using standard templates and 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 secure and unsecured devices for endpoint security testing activities Tools and Programming Languages: • Vulnerability Scanning tools like Qualys, Burp Suite, Netsparker, SQLMap, OpenVAS etc. • End-point security software such as EnCase, Tripwire, McAfee, etc. • EDR tools like SentinelOne, CrowdSec, VMware Carbon Black EDR, FireEye EDR etc. • Documentation software such as MS word, Adobe, etc. • Programming Languages for such as C++, Java, Python, Go, etc. • Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc.	

Module 17: Security Solutions for Endpoint Devices

Mapped to SSC/N0947, v1.0

Terminal Outcomes:

- Describe the tools and techniques to secure endpoint devices.
- Recommend appropriate solutions and policies to ensure network and device security.

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe various endpoint protection techniques such as encryption, mobile phone hardening, OS hardening, patch management, etc. • Explain the concepts of encryption. • Discuss the pros and cons of encryption techniques such as drive encryption, files encryption, etc. • Describe the process of mobile phone hardening. • Outline various network security methods such as firewall configuration, secure web gateway, email gateways, intrusion prevention systems, VPN encryption, etc. • Discuss browser hardening techniques to maintain browser security. • Explain the concepts of cloud security. • List popular cloud security solutions. • Discuss the best practices and regulations related to security of networks and endpoint devices.	• Demonstrate how to identify and implement the best encryption technique for sample endpoint devices. • Demonstrate the procedure to prioritize the events and processes required for maintaining devices security. • Perform mobile phone hardening using sample devices. • Demonstrate the methods to maintain internet and browser security. • Recommend suitable policies and device and network safeguarding techniques, including firewall configuration, intrusion prevention, device control, browser settings, etc., for sample 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)
- Samples of secure and unsecured devices for endpoint security testing activities

Tools and Programming Languages:

- End-point security software such as EnCase, Tripwire, McAfee, etc.
- EDR tools like SentinelOne, CrowdSec, VMware Carbon Black EDR, FireEye EDR etc.
- Encryption tools such as GnuPG, VeraCrypt, LUKS, PeaZip, etc.
- Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc.

Module 18: Monitoring and Data Collection

Mapped to SSC/N0948,v1.0 and SSC/N0949, v1.0

Terminal Outcomes:

- Apply data monitoring methods and tools to detect potential security threats

Duration (In Hours): *10:00*	**Duration (In Hours)**: *20:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe the log types and log interpretation methods. • Explain the methods of collecting logs and security alerts data. • List popular tools for monitoring network traffic and analyzing it. • Discuss the importance of reviewing organizational standards, manuals, and checklists in performing activities related to security operations	• Demonstrate the usage of specified monitoring and data collection tools. • Apply telemetry monitoring to identify security issues. • Demonstrate the log collection process from various devices and applications using specified tools. • Perform time stamping and server synchronization across logs. • Demonstrate the process of monitoring organizational traffic and logs using Security Information and Event Management (SIEM) tools. • Demonstrate the usage of common external information sources such as CND vendor sites, CERT, SANS, etc in determining security issues.
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 applications Tools and Programming Languages: • Security Methodologies and Vulnerability Frameworks like OWASP Top 10, PTES, MITRE ATT&CK etc. • SIEM tools like IBM QRadar, SolarWinds, ArcSight, Splunk etc. • Operating Systems like Kali Linux, Parrot OS, Windows, macOS etc. • Monitoring tools such as Prometheus, Nagios, Icinga, etc. • Log Analysis tools such as Nagios, ELK Stack, Graylog, etc. • Ticketing tools like JIRA, ServiceNow, Remedy etc. • Network Protocols like TCP/IP, UDP, DNS, DHCP, IPSEC, HTTP etc.	

Module 19: Basic Analysis

Mapped to SSC/N0948,v1.0 and SSC/N0949, v1.0

Terminal Outcomes:

- Perform log analysis, network traffic analysis, and event correlation to identify anomalous activities and potential cyber threats

Duration (In Hours): *10:00*	**Duration (In Hours)**: *20:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the process of identifying potential threats based on commonly observed trends and patterns. • Describe strategies to assess the cyber health of information system. • Check issues/gaps in the security posture of information system. • Describe threat analysis processes such as log analysis, packet analysis, event/ data correlation, etc. • Discuss the role of CND personnel in validating network alerts. • Explain the process of documenting the results of the monitoring, incident logging and log/event analysis.	• Demonstrate the methods to analyse network traffic and identify anomalous activity and potential threats to network resources of a sample information system. • Demonstrate the process of implementing threat analysis processes such as log analysis, event analysis, etc. to determine security issues. • Demonstrate the procedure to categorise/prioritize identified risks based on their potential impact and stipulated policies.
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 applications Tools and Programming Languages: • Security Methodologies and Vulnerability Frameworks like OWASP Top 10, PTES, MITRE ATT&CK etc. • SIEM tools like IBM QRadar, SolarWinds, ArcSight, Splunk etc. • Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc. • Monitoring tools such as Prometheus, Nagios, Icinga, etc. • Log Analysis tools such as Nagios, ELK Stack, Graylog, etc. • Ticketing tools like JIRA, ServiceNow, Remedy etc. • Traffic Analysis tools such as Wireshark, Nagios Core, NetXMS, etc. • Network Protocols like TCP/IP, UDP, DNS, DHCP, IPSEC, HTTP etc.	

Module 20: First Response to a Cyber Crime Incident

Mapped to SSC/N0950 , v1.0

Terminal Outcomes:

- Describe the processes related to initial response during a cyber incident.

Duration (In Hours): *02:50*	**Duration (In Hours)**: *05:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe the due diligence processes related to cyber investigation such as permissions, prevention of unauthorized access, etc. • List potential sources of data or evidence in a sample cyber incident. • Describe various digital forensic process models such as the 4 step-procedure, triage process model, etc. • Explain disk-based forensics and network-based forensics. • Discuss the importance of crime scene management.	• Prepare a plan that prioritizes the sources, establishing the order in which the computing devices or records can be acquired in a sample cyber incident.
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 devices, applications, templates, and checklists used for forensic investigation Tools and Programming Languages: • Forensic tools such as SleuthKit, Encase Forensics, Nuix Investigate, etc. • Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc.	

Module 21: Search and Seizure

Mapped to SSC/N0950 , v1.0

Terminal Outcomes:

- Demonstrate the identification, preservation, and seizure of digital records for investigation of a possible breach or cybercrime.

Duration (In Hours): *02:50*	**Duration (In Hours)**: *05:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the terms: volatile and non-volatile data. • Describe potential sources of evidence such as internal/ external data storage devices, portable digital devices, etc • Describe the due diligence procedures followed during evidence collection (e.g., prevention of evidence tampering, terminating destructive software in the device, preserving data integrity, etc.) • Describe host and network-based evidence • Describe methods of protecting and concealing electronic information including locking, encryption, sealing, etc. • Explain the methods to preserve information in battery-powered devices, 3rd party sources and volatile data sources. • Describe the procedure for seizing and preserving digital evidence and maintaining chain of custody. • Discuss the importance of documenting the current state, configuration, activity history of the device, stages of evidence seizure and transfer in cyber investigation.	• Demonstrate the workflows involved in establishing a data source as evidence. • Demonstrate the processes involved in seizing and preserving digital evidence. • Demonstrate volatile data analysis (memory forensics) using forensic tools. • Conduct a preview of the contents of electronic devices. • Demonstrate the examination of sample system files. • Demonstrate the creation of duplicates/back-ups for non-volatile data. • Demonstrate methods to prevent evidence loss, alteration, degradation, destruction, etc. • Prepare documents for data/ evidence collection, including details of tools and handlers,
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 devices, applications, templates and checklists used for forensic investigation	

Tools and Programming Languages:

- Awareness of building and automating a secure Chain of Custody (CoC)
- Forensic tools such as SleuthKit, Encase Forensics, Nuix Investigate, etc.
- Open-source tools like Autopsy, Helix3, CAINE, Volatility etc.
- Correlation Software such as OpenNMS, Simple Event Correlator, etc.
- Malware Analysis tools such as OllyDbg, Volatility, etc.
- Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc.
- Data Carving tools such as Foremost, Scalpel, BulkExtractor, etc.

Module 22: Cyber Forensics Policies, Procedures, Standards & Guidelines

Mapped to SSC/N0950 , v1.0

Terminal Outcomes:

- Describe the laws, policies, standards, procedures, and guidelines related to cyber forensics

Duration (In Hours): *02:50*	**Duration (In Hours)** *05:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe the laws, standards, policies, and procedures to be followed at various stages of cyber forensics such as evidence collection, evidence preservation, evidence handover, etc. • List the standard tools, checklists and templates used in cyber forensics.	• Demonstrate the operating procedures that are applicable to cyber forensics.
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 tools/templates and checklists used in cyber incidence response/investigation	

Module 23: Data Acquisition from Storage Devices, Network Traffic and Operating Systems

Mapped to SSC/N0950 , v1.0

Terminal Outcomes:

- Explain the functionalities of forensic analysis tools.

Duration (In Hours): *02:50*	**Duration (In Hours)**: *05:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• List various tools for examining and extracting data. • Describe various methods and tools for data extraction as per the make and model of data storage device. • Describe common forensic tools configurations for data acquisition. • Describe the process for extracting network traffic data. • List the data sources for network traffic data. • Discuss the importance of OS data in cyber investigation. • Explain how to handle large binary files while extracting OS data. • Discuss the do's and don'ts of OS data extraction.	• Demonstrate the usage of tools for gathering and presenting network traffic data and their limitations. • Employ data acquisition tools as per the make and build of sample storage devices. • Demonstrate the extraction of network traffic data and monitoring of network traffic data sources. • Demonstrate how to package and transport electronic evidence. • Demonstrate how to extract OS data from binary files, especially large binary files. • Demonstrate the examination of OS data in binary files.
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 devices, applications, templates and checklists used for forensic investigation Tools and Programming Languages: • Forensic tools such as SleuthKit, Encase Forensics, Nuix Investigate, etc. • Data Carving tools such as Foremost, Scalpel, BulkExtractor, etc. • Operating Systems like Kali Linux, Parrot OS, Windows, macOS, etc.	

Module 24: Cyber Forensic Analysis

Mapped to SSC/N0950 , v1.0

Terminal Outcomes:

- Analyze the data extracted from digital/electronic forensic evidence.

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Describe the investigative procedure followed in determining the identity of attacker based on collected evidence. • Discuss the relevance of file headers, file extensions, file system time, date stamps and system and application logs in cyber investigation. • Explain the methods to detect unauthorized access. • Discuss the usage of digital evidence analysis tools (e.g., log file analysis tools, registry analysis tools, web browser analysis tools, filesystem analysis tools, memory analysis tools and CDR Analysis tools). • Describe the processes of CND incident triage including determining scope, urgency, and potential impact; identifying the specific vulnerability; making recommendations that enable expeditious remediation, etc.	• Perform analysis of data extracted from sample evidence using various forensic tools. • Perform analysis of programs and file metadata in various ways to provide insights into the capability of the system and the knowledge of the user. • Demonstrate the process of identifying the method of attack using sample network traffic data. • Demonstrate digital media scanning to detect malware/virus. • Demonstrate CND incident triage. • Demonstrate data analysis of sample call records. • Demonstrate investigation of sample emails using relevant tools. • Demonstrate the use of evidence and assumptions regarding missing data in drawing conclusions. • Demonstrate how to safeguard devices and relevant information for the application of physical forensic examinations.
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 devices, applications, templates and checklists used for forensic investigation Tools and Programming Languages: • Forensic tools such as SleuthKit, Encase Forensics, Nuix Investigate, etc. • Decryption tools such as Alcatraz, TeslaCrypt, etc.	

- Correlation Software such as OpenNMS, Simple Event Correlator, etc.
- Malware Analysis tools such as OllyDbg, Volatility, etc.
- Data Carving tools such as Foremost, Scalpel, BulkExtractor, etc.
- Programming Languages such as Python, Java, C++, etc.
- Threat Intelligence tools like Anomali ThreatStream, Palo Alto Networks AutoFocus, LookingGlass etc.

Module 25: Analysis Tools

Mapped to SSC/N0950 , v1.0

Terminal Outcomes:

- Explain the functionalities of forensic analysis tools.

Duration (In Hours): *05:00*	**Duration (In Hours)**: *10:00*
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Discuss the usage of digital evidence analysis tools (e.g., log file analysis tools, registry analysis tools, web browser analysis tools, filesystem analysis tools, memory analysis tools and CDR Analysis tools). • List popular evidence analysis tools and data visualization tools.	• Demonstrate the functionalities of digital evidence analysis tools. • Prepare data visualizations for forensic analysis (when applicable) suing 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 devices, applications, templates and checklists used for forensic investigation Tools and Programming Languages: • Forensic tools such as SleuthKit, Encase Forensics, Nuix Investigate, etc. • Threat Intelligence tools like Anomali ThreatStream, Palo Alto Networks AutoFocus, LookingGlass etc. • Correlation Software such as OpenNMS, Simple Event Correlator, etc. • Malware Analysis tools such as OllyDbg, Volatility, etc. • Log Analysis tools such as Nagios, ELK Stack, Graylog, etc. • Data Visualization tools like Tableau, PowerBI etc.	

Annexure

Trainer Requirements

1.	**Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	Graduate in Engineering/Technology/ Statistics/ Mathematics/Computer Science with Minimum 5 years of relevant experience and 2 years of full-time training experience in relevant field
2.	**Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	Graduate in Engineering/Technology/ Statistics/ Mathematics/Computer Science with Minimum 5 years of relevant experience and 2 years of full-time training experience in relevant field
3.	**Tools and Equipment Required for the Training**	☒Yes ☐No *(If "Yes", details to be provided in Annexure)*
4.	**In Case of Revised Qualification, details of Any Upskilling Required for Trainer**	NA

Assessor Requirements

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	Graduate in Engineering/Technology/ Statistics/ Mathematics/Computer Science with Minimum 5 years of relevant experience and 2 years of full-time training experience in relevant field
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines), (wherever applicable)*	Graduate in Engineering/Technology/ Statistics/ Mathematics/Computer Science with Minimum 5 years of relevant experience and 2 years of full-time training experience in relevant field
3.	**Lead Assessor's/Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	Graduate in Engineering/Technology/ Statistics/ Mathematics/Computer Science with Minimum 5 years of relevant experience and 2 years of full-time training experience in relevant field
4.	**Assessment Mode** *(Specify the assessment mode)*	Online or Offline
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.

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 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
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
OS	Operating System
PwD	Persons with Disability
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
RDBMS	Relational Database Management System
SDLC	Software Development Lifecycle
OWASP	Open Web Application Security Project
OSSIM	Open Source Security Information and Event Management System
CRM	Customer Relationship Management
VAPT	Vulnerability Assessment and Penetration Testing
PC	Performance Criteria