
Model Curriculum

Analyst Application Security

SECTOR: IT-ITeS

SUB-SECTOR: IT Services

OCCUPATION: Information/Cyber Security

REF ID: SSC/Q0903

NSQF LEVEL: 7



Certificate

COMPLIANCE TO QUALIFICATION PACK – NATIONAL OCCUPATIONAL STANDARDS

is hereby issued by the

IT – ITES SECTOR SKILL COUNCIL NASSCOM

for

SKILLING CONTENT : PARTICIPANT HANDBOOK

Complying to National Occupational Standards of
Job Role/ Qualification Pack: 'Analyst – Application Security' QP No. 'SSC/Q0903NSQF Level 7'

Date of Issuance: April 9th, 2016

Valid up to*: April 10th, 2018

**Valid up to the next review date of the Qualification Pack or the
'Valid up to' date mentioned above (whichever is earlier)*

Authorised Signatory
(IT – ITES Sector Skill Council NASSCOM)

TABLE OF CONTENTS

1. Curriculum.....	01
2. Trainer Prerequisites.....	07
3. Annexure: Assessment Criteria.....	08

Analyst Application Security

CURRICULUM / SYLLABUS

This program is aimed at training candidates for the job of a “Analyst Application Security”, in the “IT-Services” Sector/Industry and aims at building the following key competencies amongst the learner

Program Name	Analyst Application Security		
Qualification Pack Name & Reference ID. ID	Analyst Application Security SSC/Q0903		
Version No.	1.0	Version Update Date	
Pre-requisites to Training	<ul style="list-style-type: none"> • Diploma in Engineering (with 1 year experience) or Bachelor's Degree in Science/Technology/Computers • 0-2 years of work experience/internship in security 		
Minimum Job Entry Age	<ul style="list-style-type: none"> • 18 years 		
Training Outcomes	<p>After completing this programme, participants will be able to:</p> <ol style="list-style-type: none"> 1. SSC/N0909 (Identify and analyze exposures and weaknesses in applications and their deployments) 2. SSC/N0910 (Harden application and deployment configurations for minimizing exposure and vulnerabilities) 3. SSC/N0911 (Monitor applications and solutions deployed for possible breaches and compromises) 4. SSC/N9001 (Manage your work to meet requirements) 5. SSC/N9002 (Work effectively with colleagues) 6. SSC/N9003 (Maintain a healthy, safe and secure working environment) 7. SSC/N9004 (Provide data/information in standard formats) 8. SSC/N9005 (Develop your knowledge, skills and competence) 		

This course encompasses 3 out of 3 National Occupational Standards (NOS) of “Analyst Application Security” Qualification Pack issued by “IT-ITeS SSC”.

Sr. No.	Module	Key Learning Outcomes	Equipment Required
1	<p>IT-ITES/BPM Industry – An Introduction</p> <p>Theory Duration (hh:mm) 18:00</p> <p>Practical Duration (hh:mm) 04:00</p> <p>Corresponding NOS Code The introduction is not based on any NOS, however is important in order to understand the context of the course and the role.</p>	<ul style="list-style-type: none"> • Explain relevance of the IT-ITES industry • State the various sub-sectors in the IT-ITES sector • Explain the relevance of IT services sector • A General Overview of the IT-BPM Industry • The organisations within IT-BPM Industry • The sub-sectors within the IT BPM Industry 	<ul style="list-style-type: none"> • Whiteboard and Markers • LCD Projector and Laptop for presentations • Lab equipped with the following: • PCs/Laptops • Internet with WiFi (Min 2 Mbps Dedicated) • Networking Equipment- Routers & Switches • Chart paper and sketch pens
2	<p>IT Services – An Introduction</p> <p>Theory Duration (hh:mm) 01:45</p> <p>Practical Duration (hh:mm) 01:00</p> <p>Corresponding NOS Code The introduction is not based on any NOS, however is important in order to understand the context of the course and the role.</p>	<ul style="list-style-type: none"> • State the various occupations and tracks in the IT-ITES sector • General Overview of the IT Services Sub-Sector • Profile of the IT Services Sub-Sector • Key Trends in the IT Services Sub-Sector • Roles in the IT Services Sub-Sector 	<ul style="list-style-type: none"> • Whiteboard and Markers • LCD Projector and Laptop for presentations • Lab equipped with the following: • PCs/Laptops • Internet with WiFi (Min 2 Mbps Dedicated)
3	<p>Information/Cyber Security – An Introduction</p> <p>Theory Duration (hh:mm)</p>	<ul style="list-style-type: none"> • Explain the relevance of cyber security in the society • Explain the role of an Analyst – Application Security and their key responsibilities • List the range of skills and 	<ul style="list-style-type: none"> • Lab equipped with the following: • PCs/Laptops • Internet with WiFi (Min 2 Mbps Dedicated)

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	<p>03:00</p> <p>Practical Duration (hh:mm) 03:00</p> <p>Corresponding NOS Code The introduction is not based on any NOS, however is important in order to understand the context of the course and the role.</p>	<p>behavior, expected from Analyst – Application Security</p> <ul style="list-style-type: none"> List the responsibilities of an Analyst – Application Security State the growth opportunities for an Analyst – Application Security General Overview of Information/cyber security and its Roles Career Map for Information/cyber security 	<ul style="list-style-type: none"> Whiteboard and Markers Chart paper and sketch pens
4	<p>Fundamental Concepts</p> <p>Theory Duration (hh:mm) 35:00</p> <p>Practical Duration (hh:mm) 30:00</p> <p>Corresponding NOS Code SSC/N0909</p>	<ul style="list-style-type: none"> relevant networking concepts, devices and terminologies standard Systems Development Lifecycle (SDLC) practices and process basic cyber security concepts the enterprise information technology (IT) architecture Information Technology Architecture what are applications, types of applications and common application security requirements the basic functionalities of the applications, hardware and/or access rights that are used by the customers application / database layer intrusion detection / prevention appliance 	<ul style="list-style-type: none"> Whiteboard and Markers LCD Projector and Laptop for presentations Lab with key devices, software and hardware in a large network. Should include but not be limited to- application of multiple networking topology; use of various Network Protocols; bandwidth management tools; application of host network access controls; hubs; switches; routers; bridges; servers; transmission media IDS/IPS; application of SSL, VPN, 2FA, Encryption, etc.
5	<p>Application vulnerabilities</p> <p>Theory Duration (hh:mm) 20:00</p> <p>Practical Duration (hh:mm) 15:00</p>	<ul style="list-style-type: none"> explain what applications are state key vulnerabilities to applications explain overall process of identification of these vulnerabilities explain how hardware and software vulnerabilities can be identified and resolved describe application/ database 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Access to various samples of applications of each category including various types of computer applications, mobile

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	<p>Corresponding NOS Code SSC/N0909</p>	<p>layer intrusion detection/prevention appliance</p>	<p>applications and cloud applications.</p> <ul style="list-style-type: none"> • Provision for online research in the lab for all students • At least two subject matter experts from the industry in the field of application security • Samples of secure applications and open source code scanning tools.
6	<p>Identification of Vulnerabilities</p> <p>Theory Duration (hh:mm) 12:00</p> <p>Practical Duration (hh:mm) 06:00</p> <p>Corresponding NOS Code SSC/N0909</p>	<ul style="list-style-type: none"> • View the system as an adversary <ul style="list-style-type: none"> ○ gather preliminary information about an application through manual documentation review ○ gather web based information through the use of automated tools and techniques ○ check the source code of a web application manually for security issues ○ collate application information security controls from various internal and external sources ○ collate information about an application with respect to industry trends through various sources ○ gather information related to application patching and its interdependencies with IT infrastructure requirements. ○ describe and use code scanning toolsets, such as Fortify and Ounce • Characterise the system <ul style="list-style-type: none"> ○ evaluate the criticality of information by taking into 	<ul style="list-style-type: none"> • Whiteboard and markers • LCD projector and laptop for presentations • Provision for online research in the lab for all students • Access to various samples of applications of each category including various types of computer, mobile, and cloud applications • Samples of secure applications • Open source code scanning tools and their tutorials • Access to secure and unsecured applications for practicing penetration testing activities • Access to public databases and vulnerability sharing clubs, e.g., <ul style="list-style-type: none"> • Bugtraq • National Institute of Standards and Technology (NIST) NVB, • United States Computer Emergency Readiness Team (US-CERT),

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		<p>consideration various factors</p> <ul style="list-style-type: none"> ○ identify the application type/ category by considering various factors ○ identify the dependency an application has with in-house/ outsourced/ third party/ client applications ○ establish the application functionality and connectivity, and understand how it works ○ review application design and architecture to ensure that appropriate security requirements are enforced ○ explore potential threats by using threat scenarios from various sources <ul style="list-style-type: none"> • Modelling the system <ul style="list-style-type: none"> ○ explore potential threats by using threat scenarios from various sources ○ efficiently isolate root causes and identify fixes by including contextual information, like architectural composition, exploitation methods, and probabilities of exposure ○ develop an application tracker with respect to risk exposure, and any application deficiency identified in the past capturing relevant information ○ validate data to identify false positives and individual vulnerabilities ○ categorise vulnerabilities and identify extent of vulnerability including level of weakness and 	<ul style="list-style-type: none"> • Open Source Vulnerability Database (OSVDB), etc.

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		<p>sensitivity of information</p> <ul style="list-style-type: none"> ○ identify the root cause of vulnerabilities ○ evaluate vulnerabilities that are discovered from their relevance, root causes, risk criticality, and corresponding mitigation methods based various factors • Application penetration testing <ul style="list-style-type: none"> ○ plan for penetration testing covering various parameters ○ test applications using various testing methods ○ use automatic scanning technologies 'black box testing' that sends malformed inputs to an application and scrutinises responses for vulnerabilities and unexpected behaviour ○ conduct manual tests that use human intelligence to guide the penetration steps can uncover hard-to-locate errors, and often more accurately reflect actions of an actual attacker ○ capture the needs and requirements required to secure applications in designated format during the application life cycle ○ capture application security requirements stipulated by clients and external stakeholders ○ document the security requirements in a structured report for easy reference and knowledge ○ document information and activities at every step to 	

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		<p>provide an audit trail</p> <ul style="list-style-type: none"> ○ secure storage of data collected during the assessment, including vulnerabilities, analysis results, and mitigation recommendations ● use tools that focus on protocol penetration testing 	
7	<p>Threat/ Vulnerability Analysis</p> <p>Theory Duration (hh:mm) 10:00</p> <p>Practical Duration (hh:mm) 05:00</p> <p>Corresponding NOS Code SSC/N0909</p>	<ul style="list-style-type: none"> ● Efficiently isolate root causes and identify fixes by including contextual information, like architectural composition, exploitation methods, and probabilities of exposure ● Develop an application tracker with respect to risk exposure, and any application deficiency identified in the past capturing relevant information ● Validate data to identify false positives and individual vulnerabilities ● Categorise vulnerabilities and identify extent of vulnerability including the level of weakness and sensitivity of information ● Identify the root cause of vulnerabilities ● Evaluate vulnerabilities that are discovered from their relevance, root causes, risk criticality, and corresponding mitigation methods based on various factors ● Capture application security requirements stipulated by clients and external stakeholders ● Document security requirements in a structured report for easy reference and knowledge ● Document information and activities at every step to provide an audit trail ● Secure storage of data collected during the assessment, including 	<ul style="list-style-type: none"> ● Whiteboard and markers ● LCD projector and laptop for presentations ● Provision for online research in the lab for all students ● Access to list of vulnerabilities and exposures identified in the application by participants in the activities of previous topic. ● Open source tools in the for the above-mentioned activities ● Provision for online research for all participants ● Sample templates for the above-mentioned points ● Provision of software, such as word processors, spreadsheets, etc. for preparing reports for all participants.

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		vulnerabilities, analysis results, and mitigation recommendations	
8	<p>Cyber Security Policies, Procedures, Standards & Guidelines</p> <p>Theory Duration (hh:mm) 15:00</p> <p>Practical Duration (hh:mm) 32:00</p> <p>Corresponding NOS Code SSC/N0909</p>	<ul style="list-style-type: none"> relevant legislation, standards, policies, and procedures followed in a company organisational systems, procedures and tasks/ checklists within the domain and how to use the same operating procedures that are applicable to the system(s) being used, typical response times and service times related to own work area OWASP tools and methodologies standard tools and templates available and how to use the same 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Provision for online research in the lab for all students Access to free OWASP tools and methods and their tutorials Around 2-3 computer applications, 2-3 mobile applications and 2-3 web applications
9	<p>Technological Developments in Application Security</p> <p>Theory Duration (hh:mm) 05:00</p> <p>Practical Duration (hh:mm) 15:00</p> <p>Corresponding NOS Code SSC/N0909</p>	<ul style="list-style-type: none"> importance of technological upgradation in cyber security next generation techniques for controlling advanced threats to applications improved ways of preventing remote applications by being compromised 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Provision for online research in lab for all students Access to free OWASP tools and methods and their tutorials Around 2-3 computer applications, 2-3 mobile applications and 2-3 web applications
10	<p>Fundamental Concepts</p> <p>Theory Duration (hh:mm) 15:00</p> <p>Practical Duration (hh:mm)</p>	<ul style="list-style-type: none"> Identify all web servers and web applications on a network Work on various operating systems Work with word processors, spreadsheets and presentations Do HTTP and web programming Read and write coded scripts 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Lab with provision for online research Lab with web application servers and web applications on the network One open source software,

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	30:00 Corresponding NOS Code SSC/N0910	and modify and debug programmes <ul style="list-style-type: none"> • Basic cyber security concepts • Relevant networking concepts, devices and terminologies • Standard Systems Development Life Cycle (SDLC) practices and process • Enterprise information technology (IT) architecture • Organisation’s knowledge base and how to access and update the same • What are applications, types of applications and common security requirements • Basic functionalities of applications, hardware and/or access rights • How hardware and software vulnerabilities can be identified and resolved for applications • Application/ database layer intrusion detection/ prevention appliance • CVE language, which standardises descriptions of vulnerabilities • Security solutions like Firewall, IDS/IPS, web security gateways, email security, content management, etc. • Relevant legislation, standards, policies, and procedures followed in a company • Limits of one’s role and responsibilities and who to seek guidance from • Organisational systems, procedures and tasks/checklists 	such as Django, Drupal, Ruby on Rails or Symfony called web application frameworks for writing applications

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		<p>within the domain and how to use the same</p> <ul style="list-style-type: none"> Operating procedures that are applicable to the system(s) being used, typical response times and service times related to own work area 	
11	<p>Application Hardening</p> <p>Theory Duration (hh:mm) 12:00</p> <p>Practical Duration (hh:mm) 00:00</p> <p>Corresponding NOS Code SSC/N0910</p>	<ul style="list-style-type: none"> About Application Hardening Application Hardening processes 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptops for making presentations
12	<p>Configuration Management</p> <p>Theory Duration (hh:mm) 12:00</p> <p>Practical Duration (hh:mm) 11:00</p> <p>Corresponding NOS Code SSC/N0910</p>	<ul style="list-style-type: none"> Configure application securely across environments for minimum exposure and weaknesses Configuration management Secure configuration of applications 	<ul style="list-style-type: none"> Whiteboard and markers Provision for online research in lab LCD projector and laptops for making presentations
13	<p>Web Application Secure Configuration</p> <p>Theory Duration (hh:mm) 15:00</p> <p>Practical Duration (hh:mm)</p>	<ul style="list-style-type: none"> configure web applications securely across environments for minimum exposure and weaknesses secure applications using tools and solutions, such as application testing, code review, web application firewall, etc. do HTTP and web programming 	<ul style="list-style-type: none"> Whiteboard and markers Lab with software and tools for writing secure web application configurations Sample secure web application configurations

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	15:00 Corresponding NOS Code SSC/N0910	<ul style="list-style-type: none"> read and write coded scripts and modify and debug programmes 	
14	Patch Management Theory Duration (hh:mm) 20:00 Practical Duration (hh:mm) 20:00 Corresponding NOS Code SSC/N0910	<ul style="list-style-type: none"> ensure all web servers, web applications and databases are patched as per latest guidelines check frontend and backend platforms for reported vulnerabilities and available patches or updates establish a mechanism to ensure that security updates and patches are applied on all application assets. This will help to close out issues or weaknesses that appear in the operational life cycle of an asset. establish measures for effectively patching an application, making business users aware about application vulnerability and patch requirements define strategy for management of patches and updates considering various relevant factors identify a patch management life cycle process considering various parameters integrate patch management with operational cycle of IT infrastructure management ensure that IT infrastructure processes are reengineered as per patch management requirements 	<ul style="list-style-type: none"> Whiteboard and markers Provision for online research in lab Sample patches Lab with key devices, software and hardware in a large network
15	Monitoring and Logging of	<ul style="list-style-type: none"> verify scope of application assets and system components to be 	<ul style="list-style-type: none"> Whiteboard and markers

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	<p>Application Events and Alarms</p> <p>Theory Duration (hh:mm) 25:00</p> <p>Practical Duration (hh:mm) 2500</p> <p>Corresponding NOS Code SSC/N0911</p>	<p>monitored with authorised persons</p> <ul style="list-style-type: none"> • use specified monitoring and data collection methods and tools following organisational procedures and policies • monitor application consoles using Security Information and Event Management (SIEM) tool to detect security threats and health of applications • define and establish operational processes for log management • • identify and capture all key events and activity logs as per established format using appropriate tools and infrastructure • ensure that mechanisms, such as time stamping and synchronisation of servers are utilised for time consistency among all log sources • maintain a tracker which captures inventory of incidents related to applications • define in co-ordination with seniors and incident management team process for incident/breach management plan and technical and tactical measures deployed to detect or report incidents • work on defined process for prioritisation and handling of incidents • characterise and analyse application traffic to identify anomalous activity and potential 	<ul style="list-style-type: none"> • Lab and access to SIEM tool and online tutorials. List of tasks that have to be performed

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		<p>threats</p> <ul style="list-style-type: none"> • identify trends and patterns as per standard guidelines • coordinate with enterprise wide computer network defence (CND) staff to validate network alerts • perform event correlation using information gathered to gain situational awareness and determine threat potential • categorise priority of identified risks by determining their probability of occurrence and potential impact as per organisational processes and policies • determine actions required to investigate and mitigate identified risks • raise incidents in ticketing tools if something is found suspicious during the analysis • record and categorise service request accurately as per organisational processes and policies • assign ticket to relevant persons as per the type of risk following organisational procedures • prioritise service request according to organisational guidelines • follow-up with relevant personnel for taking actions on tickets raised within agreed timelines • obtain help or advice from specialist if problem is outside his/her area of competence or 	

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		<p>experience</p> <ul style="list-style-type: none"> report results of monitoring, ticket raising and ticket closure activities using standard documentation following organisational procedures comply with relevant legislation, standards, policies and procedures monitor external data sources (e.g., computer network defence [CND] vendor sites, Computer Emergency Response Teams, SANS& Security Focus) and determine which security issues may have an impact on enterprise perform telemetry monitoring to identify security platform issues 	
16	<p>Manage your work to meet requirements</p> <p>Theory Duration (hh:mm) 50:00</p> <p>Practical Duration (hh:mm) 00:00</p> <p>Corresponding NOS Code SSC/N9001</p>	<ul style="list-style-type: none"> Understanding scope of work and working within limits of authority Work and work environment Maintaining Confidentiality 	<ul style="list-style-type: none"> Whiteboard and Markers LCD Projector and Laptop for presentations Training organization's confidentiality policy
17	<p>Work effectively with colleagues</p> <p>Theory Duration (hh:mm) 40:00</p> <p>Practical Duration (hh:mm)</p>	<ul style="list-style-type: none"> Effective Communication Working Effectively 	<ul style="list-style-type: none"> Whiteboard and Markers LCD Projector and Laptop for presentations Provision to write emails and send in the lab Lab with provision for internet, email, word processor and presentation

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	10:00 Corresponding NOS Code SSC/N9002		software <ul style="list-style-type: none"> Chart paper, markers, picture magazines and old newspapers
18	Maintain a healthy, safe and secure working environment Theory Duration (hh:mm) 18:00 Practical Duration (hh:mm) 07:00 Corresponding NOS Code SSC/N9003	<ul style="list-style-type: none"> Need for Health and Safety at Work Analyst's Role Emergency Situations Skills for Maintaining Health and Safety at Work 	<ul style="list-style-type: none"> Whiteboard and Markers LCD Projector and Laptop for presentations The training organization's current health, safety and security policies and procedures Provision for online research in the Lab A sample health and safety policy document Emergency broadcast system and mock emergency signage in the appropriate areas of the training institute
19	Provide data/information in standard formats Theory Duration (hh:mm) 38:00 Practical Duration (hh:mm) 12:00 Corresponding NOS Code SSC/N9004	<ul style="list-style-type: none"> Information and Knowledge Management How to manage data/information effectively Skills required to manage data and information effectively 	<ul style="list-style-type: none"> Whiteboard and Markers LCD Projector and Laptop for presentations Provision for online research in the lab
20	Develop knowledge, skills and competence Theory Duration (hh:mm) 21:00 Practical Duration	<ul style="list-style-type: none"> Importance of self-development Knowledge and Skills required for the job Avenues for Self-Development Planning for Self-Development 	Whiteboard and Markers <ul style="list-style-type: none"> LCD Projector and Laptop for presentations Soft copy of QP-NOS Provision for online access to all students in the lab Questionnaire and key for Honey and Mumford learning styles

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	(hh:mm) 04:00 Corresponding NOS Code SSC/N9005		

Grand Total Course Duration: **600 Hours, 0 Minutes**

(This syllabus/ curriculum has been approved by IT- ITes Sector Skills Council)

Trainer Prerequisites for Job role: "Analyst Application Security" mapped to Qualification Pack: "SSC/Q0903 v1.0"

Sr. No.	Area	Details
1	Description	
2	Personal Attributes	
3	Minimum Educational Qualifications	
4a	Domain Certification	
4b	Platform Certification	
5	Experience	

Annexure: Assessment Criteria

Assessment Criteria	
Job Role	Analyst Application Security
Qualification Pack	CSC/Q0903, v1.0
Sector Skill Council	IT-ITeS

Guidelines for Assessment:

1. Criteria for assessment for each Qualification Pack (QP) will be created by the Sector Skill Council (SSC). Each performance criteria (PC) will be assigned Theory and Skill/Practical marks proportional to its importance in NOS.
2. The assessment will be conducted online through assessment providers authorised by SSC.
3. Format of questions will include a variety of styles suitable to the PC being tested such as multiple choice questions, fill in the blanks, situational judgment test, simulation and programming test.
4. To pass a QP, a trainee should pass each individual NOS. Standard passing criteria for each NOS is 70%.
5. For latest details on the assessment criteria, please visit www.sscnasscom.com.
6. In case of successfully passing only certain number of NOS's, the trainee is eligible to take

Title of NOS/Unit/Component:

Assessment Outcomes	Assessment Criteria for Outcomes	Mark Allocation			
		Total Marks	Out of	Theory	Skills Practical
1. SSC/N0909 (Identify exposures and weaknesses in applications and their deployments)	PC1. gather preliminary information about the application through manual documentation review	100	5	2	3
	PC2. evaluate the criticality of information by taking into consideration various factors		5	1	4
	PC3. identify the application type/category by considering various factors		3	1	2
	PC4. gather web-based information through the use of automated tools and techniques		5	2	3
	PC5. establish the application functionality, connectivity, interdependency and working		5	2	3
	PC6. review application design and architecture to check that appropriate security requirements are enforced		3	1	2
	PC7. check the source code of an application manually and identify security issues		4	1	3

PC8. explore potential threats by considering threats from various sources	5	1	4
PC9. evaluate the vulnerabilities discovered for their relevance, root causes, risk criticality, and corresponding mitigation methods	4	1	3
PC10. collate application security controls from various internal and external sources	4	1	3
PC11. collate information about the application with respect to industry trends through various sources	4	1	3
PC12. gather information related to application patching and its interdependencies with IT infrastructure requirements	4	1	3
PC13. assess application vulnerability using security assessment tools	4	1	3
PC14. isolate root causes of vulnerabilities and identify fixes, by including contextual information like architectural composition, exploitation methods, and probabilities of exposure	4	1	3
PC15. validate data to identify failed false positives and individual vulnerabilities	4	2	2
PC16. categorize vulnerabilities and identify extent of vulnerability including level of weakness and sensitivity of the information	4	1	3
PC17. develop an application tracker capturing relevant information	3	1	2
PC18. plan for application penetration testing covering various parameters	4	1	3
PC19. test applications using various testing methods	5	2	3
PC20. Conduct penetration testing using automatic scanning technologies, “black box testing, as well as manual tests that use human intelligence to guide the steps	5	2	3
PC21. capture the requirements for securing applications stipulated by clients & external stakeholders in designated	4	1	3

	format during the application life cycle				
	PC22. document information and activities at every step to provide an audit trail		4	2	2
	PC23. secure storage of data collected during the assessment, including vulnerabilities, analysis results, and mitigation recommendations		4	1	3
	PC24. automate correlation of static, dynamic and interactive application security testing results		4	1	3
		Total	100	31	69
2. SSC/N0910 (Harden application and deployment configurations for minimizing exposure and vulnerabilities)	PC1. identify all web servers and web applications on the network and secure their administrative consoles	100	4	1	3
	PC2. review the list of all applications and ensure valid credentials are required to connect		3	1	2
	PC3. review list of systems and applications to identify and uninstall unauthorized instances and extraneous functionality to reduce the chance of exploitation		3	1	2
	PC4. apply access controls to applications and databases as required as per policy		5	1	4
	PC5. ensure all web servers, web applications and databases are patched as per latest guidelines		4	1	3
	PC6. ensure all follow security technical implementation guides (STIGs) to ensure compliance with best practices		3	1	2
	PC7. review logs for web attacks and identify signs of compromise		4	1	3
	PC8. implement application and database defenses such as firewalls		6	2	4
	PC9. ensure that all applications connect with least privilege		4	1	3

PC10. limit and monitor file creation in all web accessible directories	4	1	3
PC11. configure application securely across the environments for minimum exposure and weaknesses	6	2	4
PC12. secure applications using tools and solutions such as application testing, code review, web application firewall, etc	6	2	4
PC13. check frontend and backend platforms for reported vulnerabilities and available patches or updates	4	1	3
PC14. work on the established guidelines (or establish new ones with the support of a senior) for security configuration and hardening for each category of applications	4	1	3
PC15. establish mechanism and measures to ensure that security updates and patches are effectively applied on all the application assets	4	1	3
PC16. define security baseline for malware protection — at servers, endpoints and applications and their signatures updates including patch/security updates	6	2	4
PC17. make the business users aware about application vulnerability and patch requirements	4	1	3
PC18. define strategy for management of patches and updates considering various relevant factors	6	2	4
PC19. identify a patch management life cycle process considering various parameters	4	1	3
PC20. integrate patch management with the operational cycle of IT infrastructure management	5	1	4
PC21. ensure that IT infrastructure processes are reengineered as per the patch management requirements	3	1	2
PC22. research best practices in hardening applications	4	2	2

	PC23. document results of the outcome of the tools and solutions used		4	2	2
		Total	100	30	70
3. SSC/N0911 (Monitor applications and solutions deployed their security for possible breaches and compromises)	PC1. verify the scope of application assets and system components to be monitored with authorized persons	100	3	1	2
	PC2. use specified monitoring and data collection methods and tools following organisational procedures and policies		6	2	4
	PC3. monitor application consoles using Security Information and Event Management (SIEM) tool to detect security threats and health of the applications		6	2	4
	PC4. define and establish operational processes for log management		4	2	2
	PC5. identify and capture all the key events and activity logs as per established format using appropriate tools and infrastructure		6	2	4
	PC6. ensure that mechanisms such as time stamping and synchronization of servers are utilized for time consistency among all log sources		3	1	2
	PC7. maintain a tracker which captures inventory of incidents related to applications		3	1	2
	PC8. define in co-ordination with seniors and incident management team the process for incident/breach management plan and technical and tactical measures deployed to detect or report incidents		3	1	2
	PC9. work on the defined process for prioritization and handling of incidents		3	1	2
	PC10. characterize and analyze application traffic to identify anomalous activity and potential threats		6	2	4
	PC11. identify trends and patterns as per standard guidelines		5	2	3
	PC12. coordinate with enterprise-wide computer network defense (CND) staff to validate network alerts		3	1	2

PC13. perform event correlation using information gathered to gain situational awareness and determine the threat potential	4	1	3
PC14. categorize the priority of identified risks by determining their probability of occurrence and potential impact as per organizational processes and policies	5	1	4
PC15. determine actions required to investigate and mitigate identified risks	4	1	3
PC16. raise incidents in ticketing tools if something is found suspicious during the analysis	4	1	3
PC17. record and categorize the service request accurately as per organizational processes and policies	5	1	4
PC18. assign the ticket to the relevant persons as per the type of risk following organizational procedures	4	1	3
PC19. prioritize the service request according to organizational guidelines	4	1	3
PC20. follow-up with the relevant personnel for taking actions on the tickets raised within agreed timelines	3	0	3
PC21. obtain help or advice from specialist if the problem is outside his/her area of competence or experience	3	0	3
PC22. report the results of the monitoring, ticket raising and ticket closure activities using standard documentation following organizational procedures	3	1	2
PC23. comply with relevant legislation, standards, policies and procedures	2	1	1
PC24. monitor external data sources (e.g., computer network defense [CND] vendor sites, Computer Emergency Response Teams, SANS, Security Focus) and determine which security issues may have an impact on the enterprise	4	2	2
PC25. perform telemetry monitoring to identify security platform issues	4	1	3
Total	100	30	70

4. SSC/N9001 (Manage your work to meet requirements)	PC1. establish and agree your work requirements with appropriate people	100	7	0	7
	PC2. keep your immediate work area clean and tidy		12	6	6
	PC3. utilize your time effectively		12	6	6
	PC4. use resources correctly and efficiently		19	6	13
	PC5. treat confidential information correctly		7	1	6
	PC6. work in line with your organization's policies and procedures		12	0	12
	PC7. work within the limits of your job role		6	0	6
	PC8. obtain guidance from appropriate people, where necessary		6	0	6
	PC9. ensure your work meets the agreed requirements		19	6	13
	Total	100	25	75	
5. SSC/N9002 (Work effectively with colleagues)	PC1. communicate with colleagues clearly, concisely and accurately	100	20	0	20
	PC2. work with colleagues to integrate your work effectively with theirs		10	0	10
	PC3. pass on essential information to colleagues in line with organizational requirements		10	10	0
	PC4. work in ways that show respect for colleagues		20	0	20
	PC5. carry out commitments you have made to colleagues		10	0	10
	PC6. let colleagues know in good time if you cannot carry out your commitments, explaining the reasons		10	10	0
	PC7. identify any problems you have working with colleagues and take the initiative to solve these problems		10	0	10
	PC8. follow the organization's policies and procedures for working with colleagues		10	0	10
	Total	100	20	80	

6. SSC/N9003 (Maintain a healthy, safe and secure working environment)	PC1. comply with your organization's current health, safety and security policies and procedures	100	20	10	10
	PC2. report any identified breaches in health, safety, and security policies and procedures to the designated person		10	0	10
	PC3. identify and correct any hazards that you can deal with safely, competently and within the limits of your authority		20	10	10
	PC4. report any hazards that you are not competent to deal with to the relevant person in line with organizational procedures and warn other people who may be affected		10	0	10
	PC5. follow your organization's emergency procedures promptly, calmly, and efficiently		20	10	10
	PC6. identify and recommend opportunities for improving health, safety, and security to the designated person		10	0	10
	PC7. complete any health and safety records legibly and accurately		10	0	10
	Total		100	30	70
7. SSC/N9004 (Provide data/information in standard formats)	PC1. establish and agree with appropriate people the data/information you need to provide, the formats in which you need to provide it, and when you need to provide it	100	13	13	0
	PC2. obtain the data/information from reliable sources		13	0	13
	PC3. check that the data/information is accurate, complete and up-to-date		12	6	6
	PC4. obtain advice or guidance from appropriate people where there are problems with the data/information		6	0	6
	PC5. carry out rule-based analysis of the data/information, if required		25	0	25
	PC6. insert the data/information into the agreed formats		13	0	13
	PC7. check the accuracy of your work,		6	0	6

	involving colleagues where required				
	PC8. report any unresolved anomalies in the data/information to appropriate people		6	6	0
	PC9. provide complete, accurate and up-to-date data/information to the appropriate people in the required formats on time		6	0	6
		Total	100	25	75
8. SSC/N9005 (Develop your knowledge, skills and competence)	PC1. obtain advice and guidance from appropriate people to develop your knowledge, skills and competence	100	10	0	10
	PC2. identify accurately the knowledge and skills you need for your job role		10	0	10
	PC3. identify accurately your current level of knowledge, skills and competence and any learning and development needs		20	10	10
	PC4. agree with appropriate people a plan of learning and development activities to address your learning needs		10	0	10
	PC5. undertake learning and development activities in line with your plan		20	10	10
	PC6. apply your new knowledge and skills in the workplace, under supervision		10	0	10
	PC7. obtain feedback from appropriate people on your knowledge and skills and how effectively you apply them		10	0	10
	PC8. review your knowledge, skills and competence regularly and take appropriate action		10	0	10
		Total	100	20	80

Model Curriculum

Consultant Network Security

SECTOR: IT-ITeS

SUB-SECTOR: IT Services

OCCUPATION: Information/Cyber Security

REF ID: SSC/Q0917

NSQF LEVEL: 8



Certificate

COMPLIANCE TO QUALIFICATION PACK – NATIONAL OCCUPATIONAL STANDARDS

is hereby issued by the

IT – ITES SECTOR SKILL COUNCIL NASSCOM

for

SKILLING CONTENT : PARTICIPANT HANDBOOK

Complying to National Occupational Standards of
Job Role/ Qualification Pack: 'Consultant Network Security' QP No. 'SSC/Qoq17' NSQF Level '8'

Date of Issuance: July 9th, 2016

Valid up to*: July 10th, 2018

**Valid up to the next review date of the Qualification Pack or the
'Valid up to' date mentioned above (whichever is earlier)*

Authorised Signatory
(IT – ITES Sector Skill Council NASSCOM)

TABLE OF CONTENTS

1. Curriculum.....	01
2. Trainer Prerequisites.....	07
3. Annexure: Assessment Criteria.....	08

Consultant Network Security

CURRICULUM / SYLLABUS

This program is aimed at training candidates for the job of a “Consultant Network Security”, in the “IT-Services” Sector/Industry and aims at building the following key competencies amongst the learner

Program Name	Consultant Network Security		
Qualification Pack Name & Reference ID. ID	Consultant Network Security SSC/Q0917		
Version No.	1.0	Version Update Date	
Pre-requisites to Training	<ul style="list-style-type: none"> • Graduate in Security/ Computer Science/ Electronics and Engineering/ Information Technology • Certification in Information Systems or related fields, Basic soft skills training (Suggested but not mandatory) • 2-5 years of work experience/ internship in information technology 		
Minimum Job Entry Age	<ul style="list-style-type: none"> • 21 years 		
Training Outcomes	<p>After completing this programme, participants will be able to:</p> <ol style="list-style-type: none"> 1. SSC/N0922 (Provide network security recommendations as per requirements) 2. SSC/N0923 (Carry out configuration review and provide recommendations for secure configuration of networks and security devices) 3. SSC/N0925 (Test, run exploits to identify vulnerabilities in networks) 4. SSC/N0918 (Maintain compliance to information security policies, regulations and standards and address risk issues) 5. SSC/N0927 (Drive interrelated cyber security actions) 6. SSC/N0928 (Manage a project team) 7. SSC/N9001 (Manage your work to meet requirements) 8. SSC/N9002 (Work effectively with colleague) 9. SSC/N9003 (Maintain a healthy, safe and secure working environment) 10. SSC/N9004 (Provide data/ information in standard formats) 11. SSC/N9005 (Develop your knowledge, skills and competence) 		

This course encompasses 3 out of 3 National Occupational Standards (NOS) of “Consultant Network Security” Qualification Pack issued by “IT-ITeS SSC”.

Sr. No.	Module	Key Learning Outcomes	Equipment Required
1	<p>IT-ITES/BPM Industry – An Introduction</p> <p>Theory Duration (hh:mm) 02:00</p> <p>Practical Duration (hh:mm) 01:00</p> <p>Corresponding NOS Code The introduction is not based on any NOS, however is important in order to understand the context of the course and the role.</p>	<ul style="list-style-type: none"> • Explain relevance of the IT-ITES industry • State the various sub-sectors in the IT-ITES sector • Explain the relevance of IT services sector • A General Overview of the IT-BPM Industry • The organisations within IT-BPM Industry • The sub-sectors within the IT BPM Industry 	<ul style="list-style-type: none"> • Whiteboard and Markers • LCD Projector and Laptop for presentations • Lab equipped with the following: <ul style="list-style-type: none"> • PCs/Laptops • Internet with WiFi (Min 2 Mbps Dedicated) • Networking Equipment- Routers & Switches • Chart paper and sketch pens
2	<p>IT Services – An Introduction</p> <p>Theory Duration (hh:mm) 02:00</p> <p>Practical Duration (hh:mm) 01:00</p> <p>Corresponding NOS Code The introduction is not based on any NOS, however is important in order to understand the context of the course and the role.</p>	<ul style="list-style-type: none"> • State the various occupations and tracks in the IT-ITES sector • General Overview of the IT Services Sub-Sector • Profile of the IT Services Sub-Sector • Key Trends in the IT Services Sub-Sector • Roles in the IT Services Sub-Sector 	<ul style="list-style-type: none"> • Whiteboard and Markers • LCD Projector and Laptop for presentations • Lab equipped with the following: <ul style="list-style-type: none"> • PCs/Laptops • Internet with WiFi (Min 2 Mbps Dedicated)
3	<p>Information/Cyber Security – An Introduction</p> <p>Theory Duration (hh:mm)</p>	<ul style="list-style-type: none"> • Explain the relevance of cyber security in the society • Explain the role of a Consultant Network Security and their key responsibilities 	<ul style="list-style-type: none"> • Lab equipped with the following: <ul style="list-style-type: none"> • PCs/Laptops • Internet with WiFi (Min 2 Mbps Dedicated)

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	<p>02:00</p> <p>Practical Duration (hh:mm) 01:00</p> <p>Corresponding NOS Code The introduction is not based on any NOS, however is important in order to understand the context of the course and the role.</p>	<ul style="list-style-type: none"> List the range of skills and behavior, expected from Consultant Network Security List the responsibilities of an Consultant Network Security State the growth opportunities for an Consultant Network Security General Overview of Information/cyber security and its Roles Career Map for Information/cyber security 	<ul style="list-style-type: none"> Whiteboard and Markers Chart paper and sketch pens
4	<p>Fundamental Concepts</p> <p>Theory Duration (hh:mm) 35:00</p> <p>Practical Duration (hh:mm) 30:00</p> <p>Corresponding NOS Code SSC/N0922</p>	<ul style="list-style-type: none"> Computer fundamentals including but not limited to hard drives, networking, and encryption Internet ports, protocols and services and their usefulness System architecture and design Basic cyber security concepts Common cyber security solutions Types of electronic evidence, devices containing electronic evidence and external connections to such devices Possible electronic evidence sources relevant networking concepts, devices and terminologies Intrusion Detection Systems Vs Intrusion Prevention Systems 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentation Lab with: <ul style="list-style-type: none"> key devices, software and hardware in a large network application of multiple networking topology; use of various network protocols; bandwidth management tools; application of host network access controls; hubs; switches; routers; bridges; servers; transmission media IDS/IPS; application of SSL, VPN, 2FA, encryption, etc. provision for software development work in the lab including software and tools
5	<p>Evaluate Functional Requirements w.r.t. Network Security</p>	<ul style="list-style-type: none"> Threats and risks concerned with an organisation's network Ways to analyse network security of an organisation 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Provision for online research work in the lab for all

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	<p>Theory Duration (hh:mm) 30:00</p> <p>Practical Duration (hh:mm) 20:00</p> <p>Corresponding NOS Code SSC/N0922</p>		<p>students</p> <ul style="list-style-type: none"> Lab with: <ul style="list-style-type: none"> o key devices, software and hardware in a large network. o application of multiple networking topology; use of various network protocols; bandwidth management tools; application of host network access controls; hubs; switches; routers; bridges; servers; transmission media IDS/IPS; application of SSL, VPN, 2FA, encryption, etc..
6	<p>Review Existing Network Security Measures</p> <p>Theory Duration (hh:mm) 20:00</p> <p>Practical Duration (hh:mm) 15:00</p> <p>Corresponding NOS Code SSC/N0922</p>	<ul style="list-style-type: none"> Review the network security by analysing levels of risk associated Identify and analyse assets, risks and threats 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Provision in lab for online access for all students Sample penetration testing report and vulnerability analysis report Network security review template Two case studies for performing RCA RCA risk matrix template Field visit for walkthrough of the network security needs, solutions and policy
7	<p>Providing Solutions and Recommendations</p> <p>Theory Duration (hh:mm) 20:00</p>	<ul style="list-style-type: none"> gather sufficient accurate information on which to determine potential costs, benefits and effectiveness of potential security solutions identify and determine the cost, potential benefits, and effectiveness of recommended 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Provision for online research in the lab for all students

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	<p>Practical Duration (hh:mm) 10:00</p> <p>Corresponding NOS Code SSC/N0922</p>	<p>security solutions, based on valid assumptions, considerations and information, including possible constraints</p> <ul style="list-style-type: none"> • prepare recommendations that have the potential to meet the security objectives of the organisation • provide details of costs, benefits, effectiveness, limitations and constraints of recommendations • provide recommendations of security solutions in an agreed format to the responsible person within agreed timescales • provide the organisation with considered advice on the implications of accepting, modifying or rejecting security recommendations 	
8	<p>Configuration Management</p> <p>Theory Duration (hh:mm) 05:00</p> <p>Practical Duration (hh:mm) 12:00</p> <p>Corresponding NOS Code SSC/N0923</p>	<ul style="list-style-type: none"> • establish a baseline configuration that represents a secure state which is also cost-effective as supportive of business requirements • importance of secure configuration management of network devices • secure configuration management activities • secure configuration measures for network devices • baseline configuration 	<ul style="list-style-type: none"> • Whiteboard and markers • Networking devices - routers, switches, firewalls and access points, etc • Access to the configuration of network devices • Information security policy with baseline configurations of the network devices provided in the same • LCD projector and laptop for presentations • Provision for online research in the lab for all students
9	<p>Organisational SecCM Policy</p> <p>Theory Duration (hh:mm) 12:00</p>	<ul style="list-style-type: none"> • provide recommendation for secure configuration policies and procedures in alignment to cyber security posture of an organisation and business 	<ul style="list-style-type: none"> • Whiteboard and markers • Information security policy with baseline configurations of the network devices provided in

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	<p>Practical Duration (hh:mm) 08:00</p> <p>Corresponding NOS Code SSC/N0923</p>	<p>requirements</p> <ul style="list-style-type: none"> importance of secure configuration management of network devices secure configuration management activities secure configuration measures for network devices 	<p>the same</p> <ul style="list-style-type: none"> Provision for online research in the lab for all students LCD projector and laptops for presentations
10	<p>Identify SecCM Tools</p> <p>Theory Duration (hh:mm) 12:00</p> <p>Practical Duration (hh:mm) 08:00</p> <p>Corresponding NOS Code SSC/N0923</p>	<ul style="list-style-type: none"> provide recommendation of appropriate solution for secure configuration management (SCM solution) as per requirements of the organisation secure configuration measures for network devices available secure configuration management (SCM) solutions (SCM) 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Provision for online research in the lab for all students
11	<p>Implementing secure configurations</p> <p>Theory Duration (hh:mm) 06:00</p> <p>Practical Duration (hh:mm) 10:00</p> <p>Corresponding NOS Code SSC/N0923</p>	<ul style="list-style-type: none"> conduct an inventory to identify the network configuration items that need to be secured characterise network resources deployed into publicly available databases and customer-facing systems, resources that have high concentrations of sensitive data, and legacy security devices identify sensitive data and transaction flows identify and record configurations of network configuration items that impact the cyber security posture of an organisation review initial configuration of network configuration items considering security vulnerabilities and threats 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Provision for online research in the lab for all students Access to network devices in the lab and their configuration files Secure configuration management policy of the training institute

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		<p>identified</p> <ul style="list-style-type: none"> • establish a baseline configuration that represents a secure state which is also cost effective as supportive of business requirements • test secure configurations prior to implementation in the production environment • diagnose issues and respond to queries from the implementation team with respect to various secure configuration processes and specifications • suggest remediation to resolve issues caused due to erroneous network device configurations 	
12	<p>Unauthorised Access to Configuration Stores</p> <p>Theory Duration (hh:mm) 04:00</p> <p>Practical Duration (hh:mm) 03:00</p> <p>Corresponding NOS Code SSC/N0923</p>	<ul style="list-style-type: none"> • ensure that stores are adequately secured • various means of protecting configuration files 	<ul style="list-style-type: none"> • Whiteboard and markers • LCD projector and laptop for presentations • Provision for online research in the lab for all students • Access to configuration stores of the training institute
13	<p>Introduction to Penetration Testing</p> <p>Theory Duration (hh:mm) 10:00</p> <p>Practical Duration</p>	<ul style="list-style-type: none"> • know penetration testing • understand types of penetration testing • learn importance of the test • understand different stages of penetration testing 	<ul style="list-style-type: none"> • Whiteboard and markers • LCD projector and laptop for presentations • Sample vulnerability scan and sample penetration test of an organisation • Provision for online research in the lab for all

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	(hh:mm) 05:00 Corresponding NOS Code SSC/N0925		students
14	Pre-Penetration Test Theory Duration (hh:mm) 20:00 Practical Duration (hh:mm) 20:00 Corresponding NOS Code SSC/N0925	<ul style="list-style-type: none"> gather information using various methods and tools define scope for the test perform active reconnaissance utilise network infrastructure scanning tools 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Sample vulnerability scan and sample penetration test of an organisation Provision for online research in the lab for all students
15	Threat Modelling and Vulnerability Scanning Theory Duration (hh:mm) 10:00 Practical Duration (hh:mm) 06:00 Corresponding NOS Code SSC/N0925	<ul style="list-style-type: none"> know different types of threats perform vulnerability analysis and scanning do network scanning perform operating system fingerprinting and version scanning know and use tools and resources 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Sample vulnerability scan and sample penetration test of an organisation Provision for online research in the lab for all students
16	The Penetration Stage Theory Duration (hh:mm) 10:00 Practical Duration (hh:mm) 07:00 Corresponding	<ul style="list-style-type: none"> exploit vulnerabilities write exploits using programming languages, like C with Python, Perl and Ruby tools penetrate into firewalls, switches and routers, application software, password and codes, log management use pivoting techniques demonstrate various possible 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Sample vulnerability scan and sample penetration test of an organisation Provision for online research in the lab for all students

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	NOS Code SSC/N0925	impacts, compromises and exposures using specialised exploitation tools	
17	Post-Penetration Theory Duration (hh:mm) 10:00 Practical Duration (hh:mm) 06:00 Corresponding NOS Code SSC/N0925	<ul style="list-style-type: none"> know about writing a test report give feedback and assign severity score eliminate a penetration test trail 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Sample vulnerability scan and sample penetration test of an organisation Provision for online research in the lab for all students
18	Basics of Mobile Network Security and Cloud Network Security Theory Duration (hh:mm) 10:00 Practical Duration (hh:mm) 06:00 Corresponding NOS Code SSC/N0925	<ul style="list-style-type: none"> know basics of mobile network security understand tools used for mobile security testing learn basics of cloud network security understand tools used for cloud network security testing 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Sample vulnerability scan and sample penetration test of an organisation Provision for online research in the lab for all students
19	Information Security Policies, Regulations and Standards Theory Duration (hh:mm) 15:00 Practical Duration (hh:mm) 12:00 Corresponding NOS Code	<ul style="list-style-type: none"> ensure that all policies and procedures are implemented and well documented file compliance reports with regulatory bodies maintain legal and regulatory compliance by researching and communicating requirements, and obtain approvals correctly follow and apply policies and standards relating to information security identity 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Provision for online research in the lab for all students sample records of organisation's enterprise information technology (IT) goals and objectives

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	SSC/N0918	<p>and access management activities</p> <ul style="list-style-type: none"> • relevant legislation, standards, policies, and procedures followed in the company • legal and regulatory guidelines applicable to business or domain that organisation is engaged in • information technology (IT) supply chain security/ risk management policies, requirements, and procedures • information Security concepts, policies, and procedures 	
20	<p>Risk Treatment</p> <p>Theory Duration (hh:mm) 10:00</p> <p>Practical Duration (hh:mm) 08:00</p> <p>Corresponding NOS Code SSC/N0918</p>	<ul style="list-style-type: none"> • communicate compliance audit and risk assessment results to specified organisational personnel • share compliance issues identified during audit with appropriate organisational personnel as per process laid out • take necessary actions for closure of risk and non-conformance issues during the lifecycle • present compliance issues identified to management for prioritising, and support risk mitigation plan • co-ordinate for ongoing monitoring of risk factors to organisational operations and assets, individuals, and other organisations • meaning of risk management, risk mitigation and risk control and what these entail • aims and objectives of risk management 	<ul style="list-style-type: none"> • Whiteboard and markers • LCD projector and laptop for presentations • Provision for online research in the lab for all students • templates for conducting and documenting risk assessment activities • Risk assessment report of an organisation

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		<ul style="list-style-type: none"> activities that are involved in management of risk procedures, tools and techniques that can be used to conduct and document risk assessment activities Risk Management Framework (RMF) requirements information technology (IT) supply chain security/ risk management policies, requirements, and procedures 	
21	<p>Maintaining Compliance</p> <p>Theory Duration (hh:mm) 20:00</p> <p>Practical Duration (hh:mm) 15:00</p> <p>Corresponding NOS Code SSC/N0918</p>	<ul style="list-style-type: none"> plan and coordinate the operational activities of a given company or organisation to guarantee compliance with governmental regulations and ordinances perform occasional internal reviews, and identify compliance problems that call for formal attention file compliance reports with regulatory bodies undertake corrective actions or implementation of controls or procedural steps for satisfying needs of compliances implement an information system disposal strategy, when needed, which executes required actions when a system is removed from service maintain quality service by establishing and enforcing organisation standards 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Provision for online research in the lab for all students
22	<p>The Organisation</p> <p>Theory Duration</p>	<ul style="list-style-type: none"> relevant legislation, standards, policies, and procedures followed in the company 	<ul style="list-style-type: none"> Whiteboard and markers LCD projector and laptop for presentations Provision for online

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	(hh:mm) 15:00 Practical Duration (hh:mm) 12:00 Corresponding NOS Code SSC/N0927	<ul style="list-style-type: none"> organisational systems, procedures and tasks/ checklists within the domain and how to use the same operating procedures that are applicable to the system(s) being used, typical response times and service times related to own work area OWASP tools and methodologies standard tools and templates available and how to use the same 	research in the lab for all students <ul style="list-style-type: none"> Organisational hierarchy and management structure diagram. Cut outs in the form of labels of the various functions and job roles Standard equipment Access to organisations for visits and provision for online research Some samples of the tools/ templates and checklists used for application vulnerability assessment and penetration testing
23	The Security Department/ Function Theory Duration (hh:mm) 12:00 Practical Duration (hh:mm) 07:00 Corresponding NOS Code SSC/N0927	<ul style="list-style-type: none"> interrelation between cyber security and security function 	<ul style="list-style-type: none"> Whiteboard and marker Chart paper and markers Provision for online research for all students
24	Interactions of Cyber Security with other Functions Theory Duration (hh:mm) 24:00 Practical Duration (hh:mm) 10:00 Corresponding NOS Code	<ul style="list-style-type: none"> relevant legislation, standards, policies, and procedures followed in a company organizational systems, procedures and tasks/ checklists within the domain and how to use the same operating procedures that are applicable to the system(s) being used, typical response times and service times related to own work area OWASP tools and methodologies 	<ul style="list-style-type: none"> Whiteboard and marker LCD projector and laptop for presentations Provision for online research in the lab for all students Case lets where Consultant NetSec needs to consult colleagues and stakeholders in relation to key decisions and activities Senior subject matter expert as guest lecturer

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	SSC/N0927	<ul style="list-style-type: none"> standard tools and templates available and how to use the same 	
25	<p>Role of a Project Manager</p> <p>Theory Duration (hh:mm) 08:00</p> <p>Practical Duration (hh:mm) 02:00</p> <p>Corresponding NOS Code SSC/N0928</p>	<ul style="list-style-type: none"> comprehend the objective of the project plan project according to the timeline 	<ul style="list-style-type: none"> Whiteboard and marker LCD projector and laptop for presentation Provision for online research in the lab for all students
26	<p>Understanding Project Objectives and Timelines</p> <p>Theory Duration (hh:mm) 06:00</p> <p>Practical Duration (hh:mm) 04:00</p> <p>Corresponding NOS Code SSC/N0928</p>	<ul style="list-style-type: none"> comprehend the objective of the project plan project according to the timeline 	<ul style="list-style-type: none"> Whiteboard and marker LCD projector and laptop for presentation
27	<p>Team Selection and Allocation of Roles and Responsibilities</p> <p>Theory Duration (hh:mm) 06:00</p> <p>Practical Duration (hh:mm) 02:00</p> <p>Corresponding</p>	<ul style="list-style-type: none"> know how to build a project team distribute tasks to team members maintain deliverables and timelines 	<ul style="list-style-type: none"> Whiteboard and marker LCD projector and laptop for presentation

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	NOS Code SSC/N0928		
28	Manage Team Members Theory Duration (hh:mm) 08:00 Practical Duration (hh:mm) 04:00 Corresponding NOS Code SSC/N0928	<ul style="list-style-type: none"> • learn how to be a: <ul style="list-style-type: none"> ○ guide; ○ motivator; ○ mediator; and ○ negotiator. • conduct and handle different situations 	<ul style="list-style-type: none"> • Whiteboard and marker • LCD projector and laptop for presentation • Provision for online research in the lab for all students
29	Monitoring and Evaluation Theory Duration (hh:mm) 08:00 Practical Duration (hh:mm) 06:00 Corresponding NOS Code SSC/N0928	<ul style="list-style-type: none"> • know monitoring and evaluation of: <ul style="list-style-type: none"> ○ team members ○ project 	<ul style="list-style-type: none"> • Whiteboard and marker • LCD projector and laptop for presentation
30	Reporting, feedback and documentation Theory Duration (hh:mm) 04:00 Practical Duration (hh:mm) 02:00 Corresponding NOS Code SSC/N0928	<ul style="list-style-type: none"> • know how to make reports • give feedback 	<ul style="list-style-type: none"> • Whiteboard and marker • LCD projector and laptop for presentation • Printers and photocopiers
31	Manage your	<ul style="list-style-type: none"> • Understanding scope of work 	<ul style="list-style-type: none"> • Whiteboard and Markers

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	<p>work to meet requirements</p> <p>Theory Duration (hh:mm) 50:00</p> <p>Practical Duration (hh:mm) 00:00</p> <p>Corresponding NOS Code SSC/N9001</p>	<p>and working within limits of authority</p> <ul style="list-style-type: none"> • Work and work environment • Maintaining Confidentiality 	<ul style="list-style-type: none"> • LCD Projector and Laptop for presentations • Training organization's confidentiality policy
32	<p>Work effectively with colleagues</p> <p>Theory Duration (hh:mm) 40:00</p> <p>Practical Duration (hh:mm) 10:00</p> <p>Corresponding NOS Code SSC/N9002</p>	<ul style="list-style-type: none"> • Effective Communication • Working Effectively 	<ul style="list-style-type: none"> • Whiteboard and Markers • LCD Projector and Laptop for presentations • Provision to write emails and send in the lab • Lab with provision for internet, email, word processor and presentation software • Chart paper, markers, picture magazines and old newspapers
33	<p>Maintain a healthy, safe and secure working environment</p> <p>Theory Duration (hh:mm) 18:00</p> <p>Practical Duration (hh:mm) 07:00</p> <p>Corresponding NOS Code SSC/N9003</p>	<ul style="list-style-type: none"> • Need for Health and Safety at Work • Analyst's Role • Emergency Situations • Skills for Maintaining Health and Safety at Work 	<ul style="list-style-type: none"> • Whiteboard and Markers • LCD Projector and Laptop for presentations • The training organization's current health, safety and security policies and procedures • Provision for online research in the Lab • A sample health and safety policy document • Emergency broadcast system and mock emergency signage in the appropriate areas of the training institute
34	<p>Provide data/information</p>	<ul style="list-style-type: none"> • Information and Knowledge Management 	<ul style="list-style-type: none"> • Whiteboard and Markers

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	<p>in standard formats</p> <p>Theory Duration (hh:mm) 38:00</p> <p>Practical Duration (hh:mm) 12:00</p> <p>Corresponding NOS Code SSC/N9004</p>	<ul style="list-style-type: none"> • How to manage data/information effectively • Skills required to manage data and information effectively 	<ul style="list-style-type: none"> • LCD Projector and Laptop for presentations • Provision for online research in the lab
35	<p>Develop knowledge, skills and competence</p> <p>Theory Duration (hh:mm) 21:00</p> <p>Practical Duration (hh:mm) 04:00</p> <p>Corresponding NOS Code SSC/N9005</p>	<ul style="list-style-type: none"> • Importance of self-development • Knowledge and Skills required for the job • Avenues for Self-Development • Planning for Self-Development 	<p>Whiteboard and Markers</p> <ul style="list-style-type: none"> • LCD Projector and Laptop for presentations • Soft copy of QP-NOS • Provision for online access to all students in the lab <p>Questionnaire and key for Honey and Mumford learning styles</p>

Grand Total Course Duration: **800 Hours, 0 Minutes**

(This syllabus/ curriculum has been approved by IT- ITeS Sector Skills Council)

Trainer Prerequisites for Job role: "Consultant Network Security" mapped to Qualification Pack: "SSC/Q0917 v1.0"

Sr. No.	Area	Details
1	Description	
2	Personal Attributes	
3	Minimum Educational Qualifications	
4a	Domain Certification	
4b	Platform Certification	
5	Experience	

Annexure: Assessment Criteria

Assessment Criteria	
Job Role	Consultant Network Security
Qualification Pack	SSC/Q917, v1.0
Sector Skill Council	IT-ITeS

Guidelines for Assessment:

1. Criteria for assessment for each Qualification Pack (QP) will be created by the Sector Skill Council (SSC). Each performance criteria (PC) will be assigned Theory and Skill/Practical marks proportional to its importance in NOS.
2. The assessment will be conducted online through assessment providers authorised by SSC.
3. Format of questions will include a variety of styles suitable to the PC being tested such as multiple choice questions, fill in the blanks, situational judgment test, simulation and programming test.
4. To pass a QP, a trainee should pass each individual NOS. Standard passing criteria for each NOS is 70%.
5. For latest details on the assessment criteria, please visit www.sscnasscom.com.

Title of NOS/Unit/Component:

Assessable Outcomes	Assessment Criteria for the Outcomes	Total Marks	Out of	Theory	Skills Practical
1. SSC/N0922 (Provide network security recommendations as per requirements)	PC1. consult with customers to evaluate functional requirements for network security	100	4	1	3
	PC2. define project scope and objectives based on customer requirements		4	1	3
	PC3. confirm availability of complete and accurate details of the security objectives		3	1	2
	PC4. Evaluate the existing network protocols and topology of users		4	2	2
	PC5. review the usage of existing network security measures, and assess risks w.r.t security objectives		4	2	2
	PC6. consult with engineering teams engaged in IT networking and network security to identify network security vulnerabilities and requirements		4	1	3
	PC7. conduct technical risk analysis, threat identification of the existing network security measures		5	2	3
	PC8. identify level of risk acceptable for business requirements by discussing with business and technical leads		4	1	3

PC9. critically interpret information and data, from both within the customer/client organisation and other sources, in order to identify network security requirements	4	1	3
PC10. research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities and security risks	4	1	3
PC11. identify and record details of constraints that may have an impact on the business and security options	3	1	2
PC12. explore potential vulnerabilities that could be technical, operational or management related	5	2	3
PC13. categorize vulnerabilities and identify extent of vulnerability including level of weakness and sensitivity of the information	4	2	2
PC14. identify the root cause of vulnerabilities	4	1	3
PC15. research options of network security solutions that match the productivity and security requirements captured	5	1	4
PC16. gather sufficient accurate information on which to determine potential costs, benefits and effectiveness of potential security solutions	3	1	2
PC17. identify and determine the cost, potential benefits, and effectiveness of recommended security solutions, based on valid assumptions, considerations and information, including possible constraints	3	1	2
PC18. prepare recommendations that have the potential to meet the security objectives of the organisation	4	1	3
PC19. provide details of costs, benefits, effectiveness, limitations and constraints of recommendations	3	1	2
PC20. provide recommendations of security solutions in an agreed format to the responsible person within agreed timescales	3	1	2
PC21. provide the organisation with considered advice on the implications of accepting, modifying or rejecting security recommendations	3	1	2
PC22. co-ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs	4	1	3
PC23. take account of the organisation's values, culture and nature of business	3	1	2
PC24. maintain the security and confidentiality of information relating to your organisation and recommendations	3	1	2

	PC25. obtain necessary approvals from the responsible persons as per organisational policy		3	1	2
	PC26. evaluate ways & means of closing weaknesses in the network		4	1	3
	PC27. maintain logs for all the activities performed		3	1	2
		Total	100	32	68
2. SSC/N0923 (Carry out configuration review and provide recommendations for secure configuration of networks and security devices)	PC1. conduct an inventory to identify the information security devices that need to be protected	100	8	2	6
	PC2. characterize network resources deployed into publicly available databases and customer-facing systems, resources that have high concentrations of sensitive data, and legacy security devices		7	2	5
	PC3. identify and record the configurations of network configuration items that impact the cyber security posture of the organization		8	3	5
	PC4. review initial configuration of network configuration items considering security vulnerabilities and threats identified		8	3	5
	PC5. provide recommendations for secure configuration measures for networks considering business requirements		9	3	6
	PC6. establish a baseline configuration that represents a secure state which is also cost-effective as supportive of business requirements		9	3	6
	PC7. provide recommendation for secure configuration policies and procedures in alignment to cyber security posture of the organization and business requirements		9	3	6
	PC8. provide recommendation of appropriate solution for secure configuration management (SCM solution) as per requirements of the organisation		9	3	6
	PC9. test secure configurations prior to implementation in the production environment		11	4	7
	PC10. diagnose issues and respond to queries from the implementation team with respect to various secure configuration processes and specifications		10	3	7
	PC11. suggest remediation actions to resolve issues caused due to erroneous network device configurations		10	2	8
		Total	98	31	67

3. SSC/N0925 (Test, run exploits to identify vulnerabilities in networks)	PC1. gather preliminary information by manually reviewing the documentation, secure coding policies, security requirements, architectural designs	100	5	2	3
	PC2. gather network information using various information gathering methods and tools		5	2	3
	PC3. define scope for the tests using Existing Security Policies & Industry Standards		3	1	2
	PC4. plan for the test while adhering to business and time constraints put by organization		4	1	3
	PC5. perform Active Reconnaissance on the target network using metadata, search engines, social engineering, dumpster diving etc. after taking adequate approvals		7	2	5
	PC6. develop a map of target environments		4	1	3
	PC7. utilize network infrastructure scanning tool to conduct comprehensive network sweeps, port scans, Operating System fingerprinting and version scanning		6	1	5
	PC8. identify live systems, open / filtered ports found, services running on these ports, mapping router / firewall rules, operating system details, network path discovery, etc.		5	2	3
	PC9. perform fingerprinting services running behind open ports and underlying operating system		7	3	4
	PC10. explore the network by pre-determined scans to find possible vulnerabilities		6	2	4
	PC11. perform social engineering using Social Engineering Toolkit(SET) to find possible security holes		7	3	4
	PC12. test the network devices by supplying invalid inputs, random strings, etc., and check for any errors or unintended behaviour in the output		6	1	5
	PC13. find exploits e.g. proof-of-concept exploit for the various vulnerabilities found		5	1	4
	PC14. identify weak entry points and high value target assets of the organization or its network		5	1	4
	PC15. identify antiviruses e.g. host-based intrusion prevention systems, web application firewalls, and other preventative technologies in the system		4	1	3
	PC16. use pivoting techniques through targeted systems		5	1	4
	PC17. demonstrate various possible impacts, compromises and exposures using specialized exploitation tools		6	2	4
	PC18. evaluate ways & means of identifying and closing weaknesses in the network		6	2	4

			4	1	3
	PC19. maintain logs for all the activities performed		4	1	3
		Total	100	30	70
4. SSC/N0918 (Maintain compliance to information security policies, regulations and standards and address risk issues)	PC1. communicate the compliance audit and risk assessment results to specified organizational personnel	100	4	1	3
	PC2. share compliance issues identified during the audit with appropriate organizational personnel as per process laid out		4	2	2
	PC3. plan and coordinate the operational activities of a given company or organization to guarantee compliance with governmental regulations and ordinances		5	2	3
	PC4. ensure that all policies and procedures are implemented and well documented		5	2	3
	PC5. perform occasional internal reviews, and identify compliance problems that call for formal attention		5	2	3
	PC6. file compliance reports with regulatory bodies		5	2	3
	PC7. take necessary actions for closure of the risk and non-conformance issues during the lifecycle		4	1	3
	PC8. present compliance issues identified to the management for prioritizing, support risk mitigation plan		5	2	3
	PC9. co-ordinate for ongoing monitoring of the risk factors to organizational operations and assets, individuals, other organizations		5	2	3
	PC10. undertake corrective actions or implementation of controls or procedural steps for satisfying needs of compliances		4	1	3
	PC11. implement an information system disposal strategy, when needed, which executes required actions when a system is removed from service		5	2	3
	PC12. maintain quality service by establishing and enforcing organization standards		4	1	3
	PC13. maintain legal and regulatory compliance by researching and communicating requirements, and obtain approvals		4	1	3
	PC14. maintain regular communication and contact with organizational head and other departments to share information and to ensure that compliance related activities are coordinated		4	1	3

	PC15. document steps undertaken during the process & outcomes of the steps taken		4	1	3
	PC16. ensure that existing compliance related processes and procedures are being followed, with sufficient documentary evidence being maintained in the event of an internal/external audit		4	1	3
	PC17. complete research assignments and deliver comprehensive but concise reports in a timely manner		5	2	3
	PC18. provide timely feedback on contracts and agreements to be issued or entered into by the organization		4	1	3
	PC19. maintain professional and technical knowledge by formal and informal means		4	2	2
	PC20. ensure that customer needs are met within SLA and meet other time and quality commitment KPIs		4	1	3
	PC21. provide guidance and suggestions as appropriate		4	1	3
	PC22. complete own assigned tasks and activities to defined standards and timelines		4	1	3
	PC23. correctly follow and apply the policies and standards relating to information security identity and access management activities		4	1	3
		Total	100	33	67
5. SSC/N0927 (Drive interrelated cyber security actions)	PC1. identify the business functions, and key stakeholders within these, and establish their interest and understanding, relevant to achieving the organisation's aims	100	4	2	2
	PC2. recognise the roles, responsibilities, interests and concerns of the stakeholders in other business functions		6	1	5
	PC3. identify all the activities, functions and operations that are attributed to security or require analysis from security perspective		4	2	2
	PC4. create an inventory of roles that are responsible, accountable and informed for activities, functions and operations in cyber security		9	3	6
	PC5. create an inventory of cyber security operations that fall into various key cyber security activities		9	3	6
	PC6. identify functions that have a joint working relationship with own function		4	2	2
	PC7. consider implication of own work on other functions		6	1	5
	PC8. discuss and consult with stakeholders from other functions in relation to key decisions and activities impacting them		7	2	5

	PC9. take agreements and track actionable of other functions for interrelated work		7	3	4
	PC10. follow up with appropriate personnel for meeting timelines and effective functioning		7	2	5
	PC11. agree on communication and documentation process with stakeholders and maintain the same		6	3	3
	PC12. identify and sort out conflicts of interest and disagreements with stakeholders, in ways that minimise damage to work and activities, and to the individuals involved and the organisation		5	2	3
	PC13. monitor and review the effectiveness of working relationships with stakeholders in other business functions, seeking and providing feedback, in order to identify areas for improvement		7	3	4
	PC14. fulfil agreements made with colleagues and stakeholders and let them know, advising them promptly of any difficulties, or where it will be impossible to fulfil agreements		7	2	5
	PC15. undertake actions agreed with stakeholders in line with the terms of any agreements made		6	2	4
	PC16. advise stakeholders of difficulties or where it will be impossible to fulfil agreed actions in line with the terms of any agreements made		6	2	4
		Total	100	35	65
6. SSC/N0928 (Manage project team)	PC1. ensure the allocation and authorisation of work to the project management team is consistent with achieving the project objectives		6	1	5
	PC2. brief team members on the project and their work allocations		15	6	9
	PC3. inform team members of changes to work allocations in an appropriate way		10	3	7
	PC4. provide appropriate support and guidance to team members		15	5	10
	PC5. monitor and assess the performance of the team against agreed objectives and work plans	100	15	5	10
	PC6. provide feedback to the team at appropriate times and locations, and in a form and manner most likely to maintain and improve their performance		12	5	7
	PC7. take effective action to manage any actual or potential conflict between team members		15	5	10
	PC8. update objectives and work plans regularly, to take account of any individual, team and organisational changes		12	2	10
		Total	100	32	68

7. SSC/N9001 (Manage your work to meet requirements)	PC1. establish and agree your work requirements with appropriate people	100	7	0	7
	PC2. keep your immediate work area clean and tidy		12	6	6
	PC3. utilize your time effectively		12	6	6
	PC4. use resources correctly and efficiently		19	6	13
	PC5. treat confidential information correctly		7	1	6
	PC6. work in line with your organization's policies and procedures		12	0	12
	PC7. work within the limits of your job role		6	0	6
	PC8. obtain guidance from appropriate people, where necessary		6	0	6
	PC9. ensure your work meets the agreed requirements		19	6	13
	Total	100	25	75	
8. SSC/N9002 (Work effectively with colleagues)	PC1. communicate with colleagues clearly, concisely and accurately	100	20	0	20
	PC2. work with colleagues to integrate your work effectively with theirs		10	0	10
	PC3. pass on essential information to colleagues in line with organizational requirements		10	10	0
	PC4. work in ways that show respect for colleagues		20	0	20
	PC5. carry out commitments you have made to colleagues		10	0	10
	PC6. let colleagues know in good time if you cannot carry out your commitments, explaining the reasons		10	10	0
	PC7. identify any problems you have working with colleagues and take the initiative to solve these problems		10	0	10
	PC8. follow the organization's policies and procedures for working with colleagues		10	0	10
	Total	100	20	80	
9. SSC/N9003 (Maintain a healthy, safe and secure working environment)	PC1. comply with your organization's current health, safety and security policies and procedures	100	20	10	10
	PC2. report any identified breaches in health, safety, and security policies and procedures to the designated person		10	0	10
	PC3. identify and correct any hazards that you can deal with safely, competently and within the limits of your authority		20	10	10
	PC4. report any hazards that you are not competent to deal with to the relevant person in line with organizational procedures and warn other people who may be affected		10	0	10
	PC5. follow your organization's emergency procedures promptly, calmly, and efficiently		20	10	10

	PC6. identify and recommend opportunities for improving health, safety, and security to the designated person		10	0	10
	PC7. complete any health and safety records legibly and accurately		10	0	10
		Total	100	30	70
10. SSC/N9004 (Provide data/information in standard formats)	PC1. establish and agree with appropriate people the data/information you need to provide, the formats in which you need to provide it, and when you need to provide it	100	13	13	0
	PC2. obtain the data/information from reliable sources		13	0	13
	PC3. check that the data/information is accurate, complete and up-to-date		12	6	6
	PC4. obtain advice or guidance from appropriate people where there are problems with the data/information		6	0	6
	PC5. carry out rule-based analysis of the data/information, if required		25	0	25
	PC6. insert the data/information into the agreed formats		13	0	13
	PC7. check the accuracy of your work, involving colleagues where required		6	0	6
	PC8. report any unresolved anomalies in the data/information to appropriate people		6	6	0
	PC9. provide complete, accurate and up-to-date data/information to the appropriate people in the required formats on time		6	0	6
				Total	100
11. SSC/N9005 (Develop your knowledge, skills and competence)	PC1. obtain advice and guidance from appropriate people to develop your knowledge, skills and competence	100	10	0	10
	PC2. identify accurately the knowledge and skills you need for your job role		10	0	10
	PC3. identify accurately your current level of knowledge, skills and competence and any learning and development needs		20	10	10
	PC4. agree with appropriate people a plan of learning and development activities to address your learning needs		10	0	10
	PC5. undertake learning and development activities in line with your plan		20	10	10
	PC6. apply your new knowledge and skills in the workplace, under supervision		10	0	10
	PC7. obtain feedback from appropriate people on your knowledge and skills and how effectively you apply them		10	0	10

	PC8. review your knowledge, skills and competence regularly and take appropriate action		10	0	10
		Total	100	20	80